krisis

Kritik der Warengesellschaft

Peter Samol

Bitcoinblase und Blockchainballyhoo

Warum Bitcoin und andere Kryptowährungen kein Geld darstellen und dieses auch nicht ersetzen können

Beitrag **1 / 2018**

Bitcoinblase und Blockchainballyhoo[1]

Warum Bitcoin und andere Kryptowährungen kein Geld darstellen und dieses auch nicht ersetzen können

Peter Samol

krisis 1/2018
Kritik der Warengesellschaft

1 Der Ausdruck »Ballyhoo« stammt aus dem Englischen und bedeutet soviel wie »Werberummel« oder »theatralische Übertreibung«.

krisis – Kritik der Warengesellschaft 1/2018

Hrsg.: Förderverein krisis – Verein für kritische Gesellschaftswissenschaft e.V.
Postfach 81 02 69 | 90247 Nürnberg

Tel. + +49 911 7056 28
Fax + +49 911 780 9542

www.krisis.org
krisisweb@yahoo.de

ISSN 2196-940X

Inhalt

Zusammenfassung

Stellen Bitcoins Geld dar? Nach Auffassung ihrer Anhänger ist das der Fall. Sie glauben sogar, dass Kryptowährungen das Zentralbankgeld problemlos ersetzen können. Dieser Text will zeigen, dass es sich dabei um eine Täuschung handelt. Dazu erklärt er zunächst in allgemeinverständlicher Weise, was Kryptowährungen überhaupt sind und wie sie funktionieren. In diesem Zusammenhang wird auch auf die Blockchain-Technologie eingegangen, welche die technische Grundlage von Bitcoin und Co. darstellt.

Anschließend geht es um die Frage, ob Kryptowährungen tatsächlich Geld darstellen. Auf Grundlage der von Ernst Lohoff entwickelten Theorie des fiktiven Kapitals und der darauf beruhenden Geldtheorie wird zunächst argumentiert, dass das Geld in kapitalistisch verfassten Gesellschaften seinen Charakter als *allgemeine Ware*, die zur Darstellungsform des Tauschwerts aller anderen, besonderen Waren wird, nur erhält, weil es selbst einen Wert darstellt, der sich auf abstrakte Arbeit zurückführen lässt. Beim im Umlauf befindlichen Zentralbankgeld handelt es sich um *Geldzeichen*, die auf die bei den Zentralbanken eingelagerte *Geldware* verweisen. Diese Rolle nahm zunächst das Gold ein, im Laufe des 20. Jahrhunderts ist dieses jedoch durch Wertpapiere ersetzt worden, die einen Anspruch auf *zukünftigen* Wert repräsentieren. Krytpowährungen hingegen sind reine Zeichen ohne jeden Wert, Zeichen, die überdies aufgrund ihres spekulativen Charakters nicht einmal die wichtigsten Geldfunktionen (Zahlungsmittel, Wertaufbewahrung, Wertmaßstab) adäquat erfüllen können. Daher stellen sie auch kein Geld dar. Der Hype um sie verweist vielmehr umgekehrt auf die sich anbahnende Krise des Zentralbankgeldes.

Einleitung

Die sogenannten Kryptowährungen sind in aller Munde. Mittlerweile gibt es über 1400 verschiedene von ihnen (so der Stand Mitte 2018), und es werden täglich mehr. Einige Menschen investieren hohe Geldbeträge darin. Mit Abstand am bekanntesten ist der *Bitcoin,* andere heißen Ether, Monero, Ripple[2] etc. Einige von ihnen sind bereits auf Börsen zugelassen, an denen zuvor nur herkömmliche Finanztitel gehandelt wurden. Ermöglicht werden Kryptowährungen durch die Technologie der sogenannten *Blockchain,* ein Wort, das daher ebenfalls die Runde macht. Zugleich haben immer noch sehr viele Menschen kaum eine Vorstellung davon, was diese Begriffe eigentlich besagen bzw. wie die zugrundeliegenden Verfahren funktionieren. Viele ahnen noch nicht einmal, dass Kryptogeld und Blockchain eng miteinander zusammenhängen und dass das erstere ohne das letztere gar nicht funktionieren würde.[3]

Aus welchem Grund erfreuen sich Kryptowährungen eigentlich einer so großen Beliebtheit? Für ihre Anhänger spielt vor allem das Moment *Dezentralisierung* eine Rolle. Während das herkömmliche Geld heutzutage von den staatlichen Notenbanken herausgegeben wird – weswegen es auch als *Zentralbankgeld* bezeichnet wird –, übt niemand eine zentrale Kontrolle auf die Kryptowährungen aus. In dieser Tatsache sehen die Anhänger des Kryptogeldes eine Analogie zum Gold, das laut Hosp[4] (2018, S. 38) »automatisch dezentral geregelt« war.

[2] Genau genommen ist »Ripple« der Name einer Blockchain, und die darauf beruhende Kryptowährung heißt eigentlich »XRP«, aber selbst auf Online-Börsen wird diese als »Ripple« bezeichnet. Bei vielen anderen Kryptowährungen verhält es sich ähnlich.

[3] Umgekehrt spielen auch die Kryptowährungen auf praktisch allen Blockchains eine tragende Rolle, und es ist nicht abzusehen, wie eine Blockchain ohne eigene Kryptowährung funktionieren könnte.

[4] Der Österreicher Julian Hosp ist im deutschsprachigen Raum einer der bekanntesten Promotoren für die breite Einführung von Kryptowährungen. Über sich selbst sagt er: »Es ist zu meiner Mission geworden, den Menschen verstehen zu helfen, was Kryptowährungen sind und wie sie funktionieren, um bis 2025 mit diesem Thema die finanziellen Möglichkeiten von mindestens einer Milliarde Menschen zu erweitern« (Hosp 2018, S. 24).

Beim Gold bedurfte es keiner zentralen Organisation, denn es war einfach vorhanden bzw. wurde gefunden und hatte einen Wert, der von allen Beteiligten anerkannt wurde. In einer ähnlichen Weise ist angeblich Kryptogeld offen für jedermann. In beiden Fällen greifen außerdem staatliche Verbote und Anordnungen nicht, denn hinter Bitcoin und Co. stehen keine Firmen und keine sonstigen Institutionen (Hosp 2018, S. 123). Sie existieren einzig und allein in Form ihrer jeweiligen Blockchain, die ihrerseits ein dezentrales System darstellt, das von niemandem gestoppt oder kontrolliert werden kann, wenn es einmal in Gang gesetzt wurde.[5] Weder beim Gold noch beim Kryptogeld müsse man daher einer zentralen Organisation Vertrauen schenken (ebd.). In vielerlei Hinsicht trägt diese Analogie allerdings nicht. So zirkulierte Gold für gewöhnlich in gemünzter Form oder in gestempelten Barren, wodurch wesentliche Eigenschaften – vor allem einheitliches Gewicht und einheitlicher Reinheitsgrad – eben doch *zentral* garantiert wurden. Der wichtigste Unterschied dürfte allerdings darin liegen, dass Gold in einer bestimmten Menge als Naturstoff vorhanden ist und sein Wert aufgrund eines langen historischen Vorlaufs allgemein gesellschaftlich anerkannt wird. Kryptowährungen sind dagegen auf eine komplexe Technologie und ganz bestimmte Verfahrenweisen angewiesen, die ihrerseits einer gut funktionierenden digitalen Infrastruktur bedürfen. In dem Moment, in dem diese technische Grundlage nicht mehr funktioniert oder – was mindestens genauso möglich ist – sich als nicht vertrauenswürdig herausstellt, ist es auch um das Vertrauen in die Kryptowährung geschehen.

Trotz des Hypes um Kryptowährungen und die Blockchaintechnologie ist – zumindest für den technischen Laien – ihre Funktionsweise nicht leicht zu verstehen. Daher soll hier zunächst versucht werden, diese in möglichst allgemeinverständlicher Weise zu erklären, denn nur dann lässt sich auch die Frage beantworten, ob es sich bei Bitcoins tatsächlich um Geld handelt, wie ihre Verfechter behaupten – oder was sie sonst sind. Im Folgenden werde ich zu diesem Zweck eine Reihe von einfachen Analogien präsentieren, anhand derer

[5] Kryptogeld ist ferner vollkommen transparent und offen für jedermann. Es ist außerdem an 24 Stunden pro Tag und sieben Tagen pro Woche zugänglich.

beides (Kryptogeld und Blockchain) sowie der Zusammenhang zwischen ihnen erklärt werden soll. Dabei gerate ich wiederholt an einen Punkt, an dem eine Analogie nicht mehr trägt. Das nehme ich dann zum Anlass, sie entsprechend zu modifizieren, bis sie erneut an ihre Grenzen stößt, wieder abgeändert werden muss und so fort. Auf diese Weise versuche ich mich schrittweise der Thematik zu nähern, um diese dann im zweiten Teil dieses Textes am Beispiel des Bitcoin – seines Zeichens der Nestor der Kryptowährungen und zugleich die erste Blockchain, die in den Live-Betrieb gegangen ist – noch einmal genauer zu erläutern; außerdem wird anhand der extrem innovativen Etherium-Blockchain eine weitere Anwendungsmöglichkeit der Blockchaintechnologie vorgestellt. Im dritten Teil wende ich mich dann der Frage zu, inwiefern »Kryptowährungen« tatsächlich Geldcharakter haben, wie ihre Anhänger behaupten. Angesichts der Tatsache, dass die Geldtheorien der etablierten Wirtschaftswissenschaften darauf keine Antwort geben können, greife ich dabei auf die jüngst von Ernst Lohoff (2018) entwickelte Geldtheorie zurück.

Im Zusammenhang mit der Theorieproduktion der Gruppe Krisis versteht sich dieser Text als Auftakt zur Erschließung eines neuen Themenfeldes. Er soll eine Grundlage für weitere vertiefende Beiträge legen und eine Diskussion insbesondere hinsichtlich der Frage, ob Kryptowährungen Geld darstellen – und falls nicht, um was es sich sonst handelt – in Gang setzen.

1. Was sind Blockchain und Kryptogeld?

1.1 Was ist eine Kryptowährung? – Erste Annäherung

Beginnen wir mit einer ersten Analogie. Man stelle sich vor, in meinem Arbeitszimmer herrscht ein totales Chaos. Weil ich keine Lust habe, mich selbst an die Arbeit zu machen, gebe ich im Internet eine Anzeige auf: Wer bereit ist, mein Arbeitszimmer aufzuräumen, darf sich zur Belohnung anschließend mit dem darin vorfindlichen Material einige bunte Zettel anfertigen, die ich ihm anschließend signiere. Mit diesen Zetteln kann er dann angeblich Dinge einkaufen, sie gegen ähnliche Zettel oder sogar gegen gesellschaftlich anerkanntes Geld eintauschen.

Mit diesem einfachen, wenn auch ziemlich absurd klingenden Beispiel hätten wir uns in einem allerersten Schritt dem Kryptogeld angenähert. Ihm entsprechen hier die bunten Zettel. Tatsächlich wird Kryptogeld zunächst dadurch geschöpft, dass jemand für einen Online-Anbieter bestimmte zuvor festgelegte Dienste verrichtet, für die er mit Fantasiegeld bezahlt wird, das allerdings nicht die Form eines Zettels, sondern die eines numerischen Code (sprich: einer komplizierten Ziffernfolge) besitzt.[6] Diese wird durch Rechenaufwand im eigenen Computer erzeugt. Die zu verrichtenden Dienste bestehen in der Regel einfach darin, dass man den eigenen Computer (und oft noch weitere Hardware)[7] für komplizierte Rechenvorgänge zur Verfügung stellt. An dieser Stelle kann

[6] Die betreffenden Ziffernfolgen werden in der Regel nicht in unserem alltäglichen Dezimalsystem (mit den Ziffern von 0 bis 9), sondern im Hexadezimalsystem dargestellt (außer den Ziffern von 0 bis 9 existieren hier sechs weitere Ziffern, wobei A für 10, B für 11 … und F für 15. steht).

[7] Die sonstige Hardware besteht in der Regel aus am Computer hängenden Servern (also weiteren Rechnern) bzw. aus zusätzlich eingebauter Rechenkapazität (sprich besonders leistungsstarken Prozessoren oder aus extra eingebauten Grafikkarten, die aber nicht zur Bilddarstellung, sondern für zusätzliche Rechenleistung genutzt werden). Die neueste Entwicklung sind hochspezialisierte Rechner (so genannte »ASIC-Rechner«), die nichts anderes können, als genau die Blockchain (meist handelt es sich dabei um die Bitcoin-Blockchain) zu berechnen, für die sie gebaut wurden – das allerdings in einem unschlagbar hohen Tempo.

bereits ein erstes Missverständnis ausgeräumt werden, das durch einen Begriff entstanden ist, der von den Anhängern des Kryptogeldes offensichtlich gewählt wurde, um die angebliche Analogie zum Gold zu suggerieren: das »Mining« (»Schürfen«). Dieser Ausdruck legt die Vorstellung nahe, dass die Herstellung von einzelnen »Coins« einer Kryptowährung einfach darin bestehe, deren Code auf dem eigenen Computer ausrechnen zu lassen und diesen dann öffentlich als jeweils neuestes Exemplar eines Bitcoins, Ether, Monero und wie die Fantasienamen der digitalen »Währungen« alle lauten, bekannt zu geben. Das ist nicht ganz richtig. Zuerst, und das ist das eigentlich Entscheidende, muss eine bestimmte »Arbeit« (im Beispiel: Zimmer aufräumen) verrichtet werden, und erst *danach* darf man sich einige neue Münzen der betreffenden Kryptowährung anfertigen. Mit anderen Worten: »Mining« besteht nicht in erster Linie aus dem Schöpfen neuer Krypto-Coins, sondern in der Erledigung von zuvor festgelegten Aufgaben, die im Rahmen einer so genannten »Blockchain« stattfinden. Dabei knüpft man an eine bereits bestehende Kette (engl. »Chain«) aus Datenblöcken (»Blocks«) an. Die Erledigung der Arbeitsaufgaben resultiert in der Erstellung eines neuen Datenblocks, den man anschließend an die bisherige Kette anhängt.

Ein »Coin« einer Kryptowährung ist also eine vom eigenen Computer hergestellte Zeichenkette, die man anfertigen darf, wenn man einen Block für eine Blockchain hergestellt hat. Die Software, die man für diesen Herstellungsprozess benötigt, ist Teil derjenigen Software, die man für die Anfertigung des betreffenden Blocks zur Verfügung gestellt bekommt. Die *Gutschrift* (im Beispiel »Zimmer aufräumen« die Signierung der selbstgemachten Zettel) der neuen Coins erfolgt allerdings erst später. Dazu weiter unten mehr, denn zunächst müssen wir uns noch genauer anschauen und besser verstehen, wie eine Blockchain funktioniert.

1.2 Was ist eine Blockchain? – Erklärung in Einzelschritten

Im Jahr 1991 ist erstmals theoretisch formuliert worden, wie eine Blockchain funktionieren kann. Praktisch umgesetzt wurde diese Idee dann 18 Jahre später, im Jahr 2009, in Form der Bitcoin-Blockchain, womit zugleich die erste Kryp-

towährung ins Leben gerufen wurde. Entwickelt wurde sie von einem gewissen Satoshi Nakamoto, was vermutlich ein Pseudonym ist; jedenfalls weiß bis heute niemand, wer eigentlich dahinter steckt – wahrscheinlich handelt es sich um eine Gruppe von Personen (Hosp 2018, S. 140). Eine Blockchain ist quasi ein öffentliches Kassenbuch, in das man Buchungen schreibt, die man anschließend nicht mehr verändern kann (Voß 2018, S. 2). Im Folgenden werde ich Schritt für Schritt erläutern, wie das funktioniert und worin die Anwendungen einer Blockchain bestehen.

Blockchain: Schritt 1

Wir wissen bereits: Um Exemplare einer Kryptowährung erschaffen zu dürfen, müssen bestimmte Aufgaben im Internet verrichtet werden, die im Rahmen einer sogenannten Blockchain stattfinden. Die zu erledigenden Aufgaben finden dabei vollständig im virtuellen Raum statt. In dieser Hinsicht hinkt das Beispiel mit dem aufzuräumenden Zimmer. Ändern wir also den Vergleich ab und nehmen wir an, ich sei Schüler, und bei der zu verrichtenden Tätigkeit geht es nicht um das Aufräumen meines Zimmers, sondern um meine Hausaufgaben, die ich nicht selbst erledigen möchte. Statt meine eigenen Hirnzellen anzustrengen, stelle ich sie stattdessen ins Internet. Wer sie für mich erledigt, darf anschließend (ähnlich wie die bunten Zettel in der ersten Analogie) eine bestimmte Menge komplizierter und fälschungssicherer Zeichenfolgen mit geldähnlicher Funktion erstellen; diese Zeichenfolgen (nennen wir sie »Kryptocoins«) werden von mir nachprüfbar anerkannt, sofern ich mit der Erledigung der Hausaufgaben zufrieden bin. Auch hier stelle ich also wieder eine Belohnung in Aussicht, die praktisch aus dem Nichts geschaffen wird.

Nun haben wir die Erledigung der Aufgaben in den virtuellen Raum verlegt. Allerdings sind wir immer noch ein gutes Stück von der Erklärung der Funktionsweise einer Blockchain entfernt. Bei ihr spielen nämlich die vorangehenden Blöcke eine entscheidende Rolle. In der Regel resultieren die neu zu erledigenden Aufgaben aus dem, was zuvor passiert ist – sprich: aus dem, was in den vorangehenden Blöcken bearbeitet wurde.

Blockchain: Schritt 2

Wir müssen das Beispiel also ein weiteres Mal modifizieren. Nehmen wir an, mein Lehrer (er sei Mathematiklehrer) vergibt die Hausaufgaben so, dass die jeweils neuen Aufgaben an die Ergebnisse der letzten Hausaufgaben anknüpfen; sprich: die Zahlen, die sich beim letzten Mal ergeben haben, sind die Grundlagen für die neuen Berechnungen. Es handelt sich hier also um eine Kette (»Chain«) von Hausaufgaben, die mit der Zeit immer länger wird. Bezeichnen wir außerdem die Hausaufgaben, die ich an einem Tag bekomme, als »Block«. Wenn ich nun meine Hausaufgaben online stelle, dann gebe ich sicherheitshalber nicht nur die aktuelle Ausgangssituation (die beim letzten Mal ausgerechneten Endergebnisse) plus die neuen Aufgabenstellungen an, sondern hänge außerdem sämtliche bisher verrichteten Hausaufgaben mit an, sodass mein virtueller Helfer die ganze Kette der bisher erledigten Hausaufgaben bei Bedarf einsehen und nachprüfen kann. Der Rest ist wie bereits gehabt: Die erledigten neuen Aufgaben stellen den neuen Block dar, der an die bisherige Kette angehängt wird, und mein Helfer erzeugt sich am Ende neue Kryptocoins in Form von Codes, die ich anerkenne, wenn alles zu meiner Zufriedenheit erledigt wurde.

Eine echte Blockchain dient allerdings nicht solchen banalen Zwecken wie der Erledigung von Hausaufgaben. Sie stellt vielmehr ein *virtuelles Buchhaltungssystem* dar, in dem Eigentumsübertragungen vorgenommen, verbindlich festgelegt und unveränderbar dokumentiert werden sollen. Bei Blockchains werden einmal erzeugte Daten unveränderbar festgehalten.[8] Das Ergebnis sind verlässliche Buchungsprotokolle, wie sie im Rechtsstaat sonst nur von Notaren gewährleistet werden. Dieses Buchhaltungssystem ist außerdem *öffentlich.* Das bedeutet, jeder interessierte Mensch, der den entsprechenden Aufwand nicht scheut, kann jederzeit eine Blockchain einsehen. Des Weiteren handelt es sich bei einer Blockchain um ein *dezentrales* Buchhaltungssystem. Das ist das eigentlich Besondere an ihr. Es gibt hier nicht einen einzigen bestimmten Dienstleister,

---

[8] Im Prinzip sind die Daten immer noch veränderbar, aber Änderungen (sprich Manipulationen oder gar Betrugsversuche) wären mit einem ungeheuer großen Aufwand verbunden, sofern sie den anderen Teilnehmern der Blockchain nicht auffallen sollen.

der die Aufgaben erledigt, sondern im Prinzip können sich alle (die die entsprechende Computersoftware benutzen, ausreichend Hardwarekapazität besitzen und den damit verbundenen Energieaufwand auf sich nehmen) hieran beteiligen. Die Betreffenden arbeiten dann um die Wette, und nur derjenige, dessen Lösung am Ende übernommen wird, darf anschließend Kryptogeld für sich erzeugen. Alle anderen gehen leer aus.

Blockchain: Fast am Ziel

Für das Hausaufgabenbeispiel (an dem ich noch ein wenig festhalten möchte) würde das bedeuten, dass ich meine Aufgaben (mitsamt der kompletten Kette der bereits erledigten alten Hausaufgaben) *öffentlich* online stelle und jeder diese Aufgaben berechnen darf.[9] Nach einer gewissen Zeit schaue ich mir die bisher angebotenen Blöcke mit den Lösungsangeboten an und suche mir dann denjenigen aus, der mir am besten gefällt. Die anderen Blöcke verfallen. Nur der »Sieger«, den ich auf diese Weise ermittelt habe, darf sich neue Währungseinheiten basteln, während alle anderen Teilnehmer leer ausgehen.

Damit wäre allerdings das *dezentrale* Moment noch nicht vom Beispiel erfasst, denn noch immer entscheide *ich* als zentrale Instanz darüber, welcher Block anerkannt wird. Daher folgt sogleich die nächste Änderung. Gehen wir davon aus, dass ich meine Hausaufgaben nicht mit einem eigenen Programm online stelle, die Belohnungscoins nicht von mir selber stammen etc., sondern dass es im Internet eine öffentliche und allen zugängliche Sammelstelle für die Erledigung von Hausaufgaben gibt, in die ich meine eigenen Aufgaben mit einstellen kann. Die Helfer im Internet erledigen hier in einem Block nicht nur meine Aufgaben, sondern eine ganze Sammlung, da auch andere ihre unerledigten Hausaufgaben hier einstellen. Der neue Block wird dabei ebenso an alte Blöcke angehängt, sodass es auch hier eine jederzeit nachverfolgbare, verbindliche Kette gibt. Wer aber entscheidet jetzt, welcher Block anerkannt wird und wer dementsprechend die Belohnung erhält? Schließlich handelt es sich um ein dezentrales System, das

9 Hoffen wir einmal stark, dass mein Mathematiklehrer nicht auf die Idee kommt, im Internet nachzuschauen, ob sich seine Schüler dort unerlaubte Hilfe beschaffen.

ohne menschliche Entscheider auskommt. Für gewöhnlich bekommt einfach der schnellste Bearbeiter die Belohnung – jedenfalls sofern er alles richtig gemacht hat, was mit bestimmten mathematischen Verfahren[10] sehr schnell nachgeprüft werden kann. Nun entscheidet also nicht eine Person (und auch sonst keine zentrale Stelle) darüber, wessen Block anerkannt wird, sondern ein Automatismus, der sich aus der Blockchain selbst ergibt.

Blockchain fertig erklärt

Jetzt sind wir der Funktionsweise einer Blockchain schon recht nahe gekommen, aber immer noch nicht am Ziel. Ab hier müssen wir die Analogie des Hausgabenbeispiels leider aufgeben. Eine typische Blockchain weist nämlich eine spezifische Besonderheit auf, die sich nirgendwo sonst findet. Um einen neuen Block in der Blockchain fertig zu stellen, reicht es keineswegs aus, einfach die gestellten Aufgaben zu erledigen. Man muss außerdem noch aus sämtlichen Elementen eines Blocks eine bestimmte Zahlenfolge – den so genannten »Proof of Work« – errechnen. Erst wenn das geschehen ist und der »Proof of Work« außerdem anerkannt wurde, ist der neue Block fertig und darf der Kette angehängt werden. Anschließend muss man den neuen Block noch online stellen (im Blockchain-Jargon »broadcasten«, was in etwa soviel bedeutet wie »veröffentlichen«) und hoffen, dass man der Schnellste ist und den dafür ausgelobten Betrag an Kryptogeld einstreichen darf.

Was sind nun die Elemente eines Blocks, die man miteinander verrechnen muss?

a) Jeder Block bekommt zunächst einen eigenen Index (eine bestimmte hexadezimale Zahlenfolge) zugewiesen; dieser Index ist sozusagen der Name des neuen Blocks.

b) Hinzu kommt ein Zeitstempel, aus dem zu entnehmen ist, zu welchem Zeitpunkt der neue Block fertiggestellt wurde. Auch er besteht aus einer Zahlenfolge.

[10] Mehr zu diesen Verfahren folgt später.

c) Des Weiteren kommt die schon bekannte Darstellung der gesamten bisherigen Kette von Blöcken einschließlich des neuen Blocks[11] hinzu. Auch aus dieser wird eine bestimmte Zahl (ein so genannter »Hash«) errechnet.

d) Last not least muss man eine Zufallszahl (eine so genannte »Nonce«[12]) mit einrechnen. Sie stellt das abschließende Element – gewissermaßen den Schlussstein – des neuen Blocks dar, der das Ergebnis vervollständigt (siehe Hosp 2018, S. 69).

Die Zahl, die sich aus der Verrechnung dieser vier Elemente ergibt, ist der »Proof of Work«. Dabei erfolgt die Verrechnung auf der Basis eines komplizierten mathematischen Verfahrens, das sehr schwer durchzuführen, aber leicht nachzuprüfen ist.[13] Dadurch ist das Verfahren extrem zeit- und energieintensiv. Das ist so gewollt, um nachträgliche Fälschungen einer Blockchain, bei denen dieses Verfahren für jeden einzelnen Block ebenfalls wieder durchlaufen werden müsste, extrem unattraktiv bzw. unmöglich zu machen. Das Ergebnis ist immer eine einzige Ziffernfolge, doch mit ihrer Herstellung ist der »Proof of Work« noch nicht abgeschlossen. Die betreffende Zahl muss nämlich auch noch eine ganz bestimmte Bedingung erfüllen, sonst wird sie nicht als gültig anerkannt und muss neu berechnet werden. Bei der Blockchain, auf welcher der Bitcoin beruht, besteht diese Bedingung darin, dass die Zahl eine bestimmte Größe

[11] In diesem neuen Block befindet sich auch die »Arbeitslast« (im Beispiel: die Hausaufgaben), die auf diese Weise selbst in die Berechnung des »Proof of Work« mit eingeht.

[12] »Nonce« ist die Abkürzung für den Ausdruck »Number Only Used Once«. Das soll im Grunde nichts anderes bedeuten, als dass man eine Zufallszahl für den einmaligen Gebrauch finden soll.

[13] Ein relativ einfaches Beispiel für eine mathematische Aufgabe, die relativ schwer zu lösen aber sehr leicht zu überprüfen ist, wäre beispielsweise die Aufgabe: »Bestimme sämtliche Primzahlen, aus denen die Zahl 91 besteht«. Man muss hier einige Zeit überlegen und probieren, um auf die Lösung »7 und 13« zu kommen. Die Überprüfung »7 * 13 = 91« ist dagegen recht schnell und einfach vollzogen. In der Kryptologie werden Aufgaben verwendet, für deren Erledigung selbst Hochleistungscomputer viele Minuten, Tage oder sogar Jahre benötigen, während die Überprüfung lediglich Sekundenbruchteile erfordert.

nicht überschreiten darf. Das sieht praktisch so aus, dass die Ziffernfolge in ein Ziffernfeld mit einer vorgegebenen Länge eingetragen wird und die ersten sieben Stellen ausschließlich Nullen aufweisen dürfen. Ist diese Bedingung nicht erfüllt, muss die Ziffernfolge neu berechnet werden. Erst wenn man eine passende Zahl gefunden hat, ist der neue Block fertiggestellt. Durch Anpassung der Bedingung für die Gültigkeit kann gesteuert werden, wie aufwendig die Berechnung des »Proof of Work« werden soll. In der Bitcoin-Blockchain wird diese Berechnung beispielsweise so angepasst, dass die Miner im Durchschnitt alle 10 Minute einen gültigen Block herstellen (Schulz 2017a, S. 104).

Der Zweck dieses aufwendigen Prüf- und Verschlüsselungsverfahrens besteht darin, Fälschungen einer bestehenden Blockchain erheblich zu erschweren. Realiter werden Blockchains für Buchungszwecke eingesetzt, bei denen es um enorme Geldbeträge und um Eigentumsverhältnisse gehen kann. Und da hört bekanntlich jeder Spaß auf. Die Verschlüsselung erfüllt hier eine wichtige Kontrollfunktion, bei der es insbesondere darum geht, öffentlich einsehbare Information verbindlich und fälschungssicher darzustellen. Da jeder Block für sich verschlüsselt wird und gleichzeitig eine Abbildung aller vorhergehenden Blöcke enthält, können auch alte Buchungen jederzeit anhand eines aktuellen Blocks eingesehen werden. Zugleich ist es enorm schwer bzw. nahezu unmöglich, diese Informationen zu fälschen, zu manipulieren oder auch nur Abschreibfehler zu begehen. Denn da jeder Block für sich verschlüsselt ist und alle vorhergehenden Blocks in den aktuellen Schlüssel mit eingerechnet werden, fallen nachträgliche Manipulationen von früheren Buchungen dadurch auf, dass eine Nachprüfung nicht zum aktuellen Schlüssel führen würde. Die Inhalte älterer Blöcke könnten nur dann unbemerkt gefälscht werden, wenn alle später erstellten Blocks zuvor entschlüsselt und neu berechnet werden. Kurz: »Wenn man die Vergangenheit ändern wollte, müsste man alle folgenden Blöcke rückgängig machen und ganz von vorn anfangen« (Hosp 2018, S. 71). Dieser Aufwand ist praktisch nicht zu schaffen, schon allein weil die anderen Miner zugleich schon dabei sind, neue Blocks herzustellen, die man ebenfalls fälschen müsste, wenn man nicht schnell genug ist. Das wäre allenfalls durch extrem schnelle und hochleistungsfähige Rechner

auf der Basis der neuesten Technologie zu schaffen. Um das zu verhindern, wird der Schwierigkeitsgrad des »Proof of Work« ständig im Gleichschritt mit der technischen Entwicklung erhöht, so dass es immer in etwa gleich schwer ist, einen Block zu fälschen (Mayer-Kuckuk 2017, S. 15).

Eine Blockchain existiert letztlich nur dadurch, dass es immer genügend Teilnehmer (sprich: Miner) gibt, die neue Blocks berechnen. Da die Miner hierzu einen großen Kostenaufwand für Rechenzeit, Energie und Hardware haben, braucht es eine Belohnung, denn sonst würde sich niemand an der Aufrechterhaltung einer Blockchain beteiligen. Diese Belohnung erfolgt in Form von Kryptogeld (Schulz 2017a, S. 104). Praktisch alle Blockchains sind daher mit irgendeiner Form digitalen Geldes verknüpft. Insofern sind Kryptogeld und Blockchaintechnologie aufeinander angewiesen: Ohne Blockchain kein Kryptogeld und ohne Kryptogeld keine Blockchain.[14]

Zuletzt muss noch eine Besonderheit erklärt werden, die sich beim Betrieb einer Blockchain recht häufig ereignet: Das Aufkommen einer so genannten Verzweigung (engl.: »Fork«). Es kann nämlich passieren, dass zwei Teilnehmer gleichzeitig einen neuen Block fertig stellen und beide in das Netzwerk der Blockchain eingestellt werden. Die beiden alternativen Blöcke existieren dann gleichzeitig. Damit nicht genug, passiert es dann sehr häufig, dass an beide dieser alternativen Blöcke eine Zeit lang jeweils weitere Blöcke angehängt werden. In diesem Fall hat sich eine Verzweigung bzw. eine »Fork« ereignet. Das könnte dann zur Folge haben, dass ein Kryptogeldbetrag im einen Zweig für eine andere Zahlung benutzt wurde als im anderen, also praktisch mit demselben Coin zweimal bezahlt wurde. So etwas darf eigentlich nicht vorkommen, denn es unterhöhlt jede Geldfunktion. Wie geht das Netzwerk nun mit solchen Verzweigungen um?

[14] Man könnte sich allenfalls eine sehr einfache und leicht zu bedienende Blockchain ohne Kryptogeldbelohnung vorstellen, die von Liebhabern oder »Idealisten« umsonst betrieben wird – diese Blockchain wäre aber sehr leicht und mit geringem Aufwand zu fälschen und daher nicht besonders sicher.

Betrachten wir im Detail, wie sich eine Verzweigung ereignet: Sobald ein »Miner« einen gültigen Block errechnet hat, schickt er ihn per Broadcast an alle anderen Mitglieder des Netzes der betreffenden Blockchain. Treffen mehrere neue Blöcke ein, können die nächsten Bearbeiter entscheiden, welchen davon sie bearbeiten. Meist nehmen sie einfach den ersten, der eingetroffen ist (Schulz 2017a, S. 105). Trudeln aber zwei alternative Blöcke derart zeitnah ein, dass beide von ihnen neue Bearbeiter finden, dann teilt sich die Blockchain zunächst in zwei Zweige auf, und an beiden wird von verschiedenen Teilnehmern weitergearbeitet. Früher oder später wird aber einer der beiden Äste spürbar länger als der andere sein. Dann wird der kürzere Zweig automatisch entfernt.[15] Für die für ungültig erklärten Blöcke gibt es keine Belohnungen (sprich: kein Kryptogeld) (ebd.). Erfahrungsgemäß braucht es maximal sechs neue Blöcke, bis so ein »Rennen« zwischen den Zweigen einer Fork entschieden ist. Daher wird das Kryptogeld erst dann ausgezahlt, wenn an einem neuen Block mindestens sechs weitere angehängt wurden. Erst dann werden auch die Arbeitsaufträge des betreffenden Blocks wirklich abgewickelt (Schulz 2017a, S. 105).[16] Forks treten relativ häufig auf, was bedeutet, dass sehr viel Energie und Rechenzeit vollkommen umsonst für Blocks verausgabt werden, die sich im falschen Zweig einer Fork befinden.

Blockchain: Kurze Zusammenfassung

Fassen wir noch einmal kurz zusammen. Eine Blockchain ist im Grunde nicht viel mehr als eine dezentrale, öffentlich einsehbare und von allen Teilnehmern anerkannte Datenbank, die aus einer Kette von Datenblöcken besteht (Schulz 2017a, S. 103). Jeder Teilnehmer (sprich Miner) einer Blockchain verfügt über das vollständige Verzeichnis der bisherigen Blöcke. Wer einen neuen Block erstellt, sendet diesen sofort an alle anderen Teilnehmer. Diese überprüfen, ob alles in Ordnung ist und beginnen dann, den nächsten Block zu berechnen.

[15] Aufgaben, die im verworfenen Zweig erledigt wurden, im anerkannten Zweig aber nicht, werden als unerledigt erkannt und in späteren Blöcken erledigt.

[16] Jedenfalls sofern es sich nicht um Kleinstbeträge handelt, die aus praktischen Gründen früher anerkannt werden (vgl. Hosp 2018, S. 72).

So wächst die Kette der Blöcke – eben die Blockchain – immer weiter. Durch die Abbildung der Vorgängerblöcke und ihre kryptographische Verkettung mittels des »Proof of Work« sind sämtliche Blöcke untereinander verknüpft und praktisch unveränderbar dokumentiert, wodurch sie sich wechselseitig vor Manipulationen bzw. Speicher- und Übertragungsfehlern schützen (ebd.). So werden nachträgliche Änderungen praktisch verhindert, und zugleich ist die Reihenfolge von Transaktionen transparent und nachvollziehbar abgebildet. An einer Blockchain kann im Prinzip jeder mitwirken, der die nötige Hardware mitbringt und den entsprechenden Energieaufwand nicht scheut. Die Teilnehmer an einer Blockchain konkurrieren um das Recht, die gestellten Aufgaben (die »Workload« eines jeden Blocks) abwickeln zu dürfen. Auf die Frage, warum sie diesen Aufwand betreiben und entsprechende Ressourcen zur Verfügung stellen, lautet die simple Antwort: Weil sie dafür mit Kryptogeld bezahlt werden.

Damit Blockchains und Kryptowährungen überhaupt funktionieren können, ist der Schutz vor Fälschungen und Manipulationen extrem wichtig. So muss etwa jederzeit vollkommen und absolut eindeutig klar sein, wo sich ein bestimmter Betrag einer Kryptowährung befindet und wem er gehört. Würde er stattdessen doppelt auftauchen oder einfach verschwinden, weil irgendjemand vergangene Zahlungsvorgänge verfälscht hat, dann wäre es um das Vertrauen in die betreffende Kryptowährung sofort geschehen. Auch die entsprechende Blockchain hätte jedes Vertrauen verspielt. Eine der hervorstechendsten Eigenschaften einer Blockchain ist daher ihre Robustheit gegen nachträgliche Änderungen, die darin begründet ist, dass sich einmal gespeicherte Daten sich nur ändern ließen, wenn man auch alle nachfolgenden Blöcke neu berechnet würden, was die nötige Rechenleistung in astronomische Höhen triebe (Schulz 2017a, S. 103). Da außerdem zeitgleich andere Teilnehmer neue Blöcke von einer günstigeren Startposition aus berechnen (nämlich vom aktuellen Block aus), müsste man mindestens doppelt so schnell sein wie alle anderen Konkurrenten, um auch nur den aktuellen Block zu manipulieren (bei allen vorherigen vervielfacht sich das notwendige Rechentempo entsprechend).

2. Verschiedene Anwendungen von Blockchains und Kryptowährungen

Es gibt zur Zeit vor allem zwei prominente Anwendungen der Blockchain-Technologie. Erstens wird sie für die Verwaltung von Finanztransaktionen eingesetzt – wobei es sich in der Regel nur um Kryptogeld handelt. Ein typisches Beispiel hierfür ist die Bitcoin-Blockchain, die nichts anderes tut, als die eigene Kryptowährung (eben den Bitcoin) zu verwalten. Zweitens gibt es noch die Abwicklung von automatisierten Verträgen – so genannten »Smart Contracts«. Dies ist eine Spezialität der sehr experimentierfreudigen Ethereum-Blockchain, die über die eigene Kryptowährung »Ether« verfügt.

2.1 Das Original: Die pure Selbstverwaltung der Bitcoin-Blockchain

Der Bitcoin war das erste Kryptogeld überhaupt und ist bis heute der Platzhirsch unter den Kryptowährungen (Hickel 2017, S. 12). Er funktioniert auf der Basis der gleichnamigen Blockchain, die ihrerseits als erste der Welt in Betrieb gegangen ist. Alles begann damit, dass der bereits erwähnte Satoshi Nakamoto im Jahr 2008 eine theoretische Lösung zur Verhinderung des »Double Spendings« (also des zweimaligen Ausgebens einer Einheit einer dezentralen digitalen Währung) veröffentlichte (Hosp 2018, S. 44) und zwar ohne dafür eine Zentralbehörde (etwa eine Bank) oder auch nur ein zentrales Verzeichnis (z.B. eine Daten-Bank) zu benötigen (Junge Linke 2012, S. 7). Dass Geld nicht mehrfach ausgegeben werden kann, ist extrem wichtig für die Erfüllung seiner Funktion. Es muss beim Bezahlen verbindlich an den jeweiligen Tauschpartner weitergereicht werden, der es anschließend besitzt, während es dem ursprünglichen Besitzer nicht mehr gehört. In seiner Veröffentlichung nahm Nakamoto jene Lösung des Double Spending-Problems vorweg, die wenig später beim Bitcoin praktisch umgesetzt wurde: Eine Mehrfachausgabe wird beim Bitcoin unter anderem dadurch verhindert, dass jeder einzelne Bitcoin zunächst einmal (genauso wie die Exemplare

anderer Kryptowährungen) in Form einer bestimmten Ziffernfolge existiert. Diese Zeichenfolge entspricht in etwa der Seriennummer eines Geldscheins. Viel wichtiger als diese Zeichenfolge ist aber die lückenlose Dokumentation der Eigentümer des betreffenden Bitcoin – von seinem Miner bis hin zum gegenwärtigen Besitzer – durch die Bitcoin-Blockchain. In dieser wird anzeigt, wer den betreffenden Coin gerade besitzt und welche Personen ihn zuvor besessen haben. Nur diese lückenlose Dokumentation macht einen Bitcoin wirklich gültig. Daher kann es ohne eine zugehörige Blockchain keinen Bitcoin (und auch sonst keine Kryptowährung) geben.

Am 3. Januar 2009 wurde der »Genesis-Block« – so wird im Blockchain-Jargon der erste Block einer Kette genannt – von Satoshi Nakamoto selbst hergestellt. Die erste Bitcoin-Transaktion erfolgte neun Tage später, als Nakamoto zehn Bitcoins an eine andere Person verschickte. Mittlerweile (Mitte 2018) existieren rund 17 Millionen Bitcoins, wobei die mögliche Gesamtzahl durch das technische Verfahren auf 21 Millionen beschränkt ist, die aber erst im Jahr 2140 erreicht werden soll (Landgraf 2018, S. 2). Zu erwähnen ist noch, dass der Bitcoin wie jede andere Währung auch über Untereinheiten verfügt, wobei einem Bitcoin die beachtliche Anzahl von 100.000.000 (hundert Millionen) »Satoshis« (nach dem Vornahmen des Erfinder-Pseudonyms) entspricht. Damit stünden derzeit ca. 230.000 Satoshis pro Erdenbürger zur Verfügung.

An der Bitcoin-Blockchain kann man auf zwei verschiedene Weisen teilnehmen. Entweder als einfacher User, der Bitcoin gegen eine gängige offizielle Währung erwirbt und anschließend damit bezahlt, handelt, spekuliert etc., oder als Miner, der dazu beiträgt, die Blockchain zu bearbeiten.[17] Als einfacher User benötigt man eine Bitcoin-Wallet (Brieftasche). Das ist ein Computerprogramm,

[17] Außer den Usern und den Minern gibt es als drittes Element noch die » Nodes« (dt.: »Knotenpunkte«). Das sind in der Regel keine Personen, sondern reine Verzeichnisse im Internet, die Informationen über User, Miner und andere Nodes enthalten. Außerdem speichern sie die gesamte Blockchain. Nodes sind lediglich als Kontrollstellen eingerichtet und tätigen selbst keine Transaktionen (siehe Hosp 2018, S. 61). Sie sind in unserem Zusammenhang nicht weiter wichtig und werden hier nur der Vollständigkeit halber erwähnt.

auf dem das eigene Bitcoin-Guthaben verzeichnet ist und das es einem außerdem ermöglicht, Bitcoins auszugeben oder zu erwerben.[18] Nun sind zwar alle Bitcoin-Transaktionen öffentlich und in der Bitcoin-Blockchain unveränderbar dokumentiert, allerdings werden die Konten nur in Form von Buchstaben-Zahlenkombinationen verzeichnet, wodurch die Nutzer anonym bleiben. Das birgt allerdings auch ein gewisses Risiko, denn wenn ein User seine Wallet verliert oder Bitcoin-Börsen gehackt werden, ist das Kryptogeld weg.

Die Miner benötigen darüber hinaus eine Software, die es ihnen ermöglicht, alte Blöcke zu überprüfen und neue zu erstellen. In den Anfängen genügte für das Bitcoin-Mining noch ein normaler Desk- oder Laptop. Heutzutage sind die darin verwendeten Computerprozessoren jedoch viel zu langsam, um im Wettrennen mit anderen Minern auch nur die geringste Chance zu haben. Ihre »Hash-Rate« beträgt nämlich »lediglich« eine Million bis drei Millionen pro Sekunde. Die Hash-Rate ist die Anzahl der Versuche pro Sekunde, einen Proof of Work zu erstellen.[19] Das Mining mit normalen Computern ist daher heute praktisch ausgestorben (Hosp 2018, S. 76). Eine Zeitlang wurde dann »GPU-Mining« betrieben; hierbei werden mehrere Grafikkarten gleichzeitig eingesetzt, die nicht zur Bilddarstellung, sondern zum Krypto-Mining verwendet werden. Dabei beträgt die Hash-Rate 30 Millionen bis 50 Millionen pro Sekunde. Für Bitcoins ist auch das inzwischen zu langsam, aber bei anderen Kryptowährungen wird häufig noch Mining auf diese Weise betrieben (ebd.). Der Standard beim Bitcoin ist heute das »ASIC-Mining«. ASIC steht für »anwendungsspezifische, integrierte Schaltkreisläufe«, die speziell für die Bitcoin-Blockchain entwickelt werden. Es gibt Firmen, deren gesamtes Geschäftmodell darin besteht, diese Computer herzustellen (ebd., S. 76 f.). Das Ergebnis sind hochspezialisierte Computer

[18] Bitcoins werden immer auf der Blockchain aufgezeichnet und bewegen sich nie von dort weg (Hosp 2018, S. 96). Eine »Wallet« verschafft einem lediglich den Zugang zu den eigenen Bitcoins, denn in ihr sind die Bitcoin-Adressen gespeichert. Was man dementsprechend verlieren kann, sind nicht die Bitcoins, sondern lediglich der Zugang zu ihnen (ebd.).

[19] Ein Mensch hätte etwa eine Hash-Rate von 0,00003 H/s (Hashes pro Sekunde) (Hosp 2018, S. 75).

(so genannte ASIC-Miner), die nichts anderes können als Bitcoin-Mining zu betreiben, dafür aber mehrere Giga- (Milliarden) oder sogar Tera- (Trillionen) Hashes pro Sekunde ausführen. Sie werden in der Regel zu Hunderten oder gar Tausenden auf riesigen Mining-Farmen in Ländern mit günstigen Strompreisen wie Island, China oder Russland eingesetzt (ebd., S. 79).[20] Selbst dann dauert es Monate und manchmal Jahre, bis sich die riesigen Investitionen amortisieren. Dabei müssen sich die Betreiber beeilen, denn da Mining-Computer sich schnell verbessern, ist die eigene Hardware sehr schnell nichts mehr wert (ebd., S. 78).[21]

Wie schon gesagt, kommen neue Bitcoins in die Welt, weil die Miner für ihre »Arbeit« entlohnt werden, wenn sie einen neuen anerkannten Block erstellt haben. Im Bitcoin-Netzwerk entstehen die neuen Bitcoins (genauso wie die entsprechenden Coins bei den anderen Kryptowährungen) also aus dem Nichts, indem die Computer am Ende aller anderen Transaktionen sich selbst nach einem bestimmten Verfahren bestimmte Zeichenketten ausrechnen dürfen, die jeweils einem Bitcoin entsprechen. Die Miner stellen dem System also die Rechenleistung ihrer starken Computer zur Verfügung und erhalten dafür Coins als Belohnung. Da das Bitcoin-System auf 21 Millionen Münzen beschränkt bleiben soll, wird die Menge der ausbezahlten Bitcoins in regelmäßigen Abständen halbiert. Dieses »Halving« (Halbierung) ist im kryptografischen Algorithmus der Bitcoin-Blockchain eingeschrieben und stellt die eigentliche (und einzige) Grundlage für die Festschreibung der Maximalzahl der Bitcoins dar. Ein Halving findet genau alle 210.000 Blöcke – das sind etwa alle vier Jahre – statt. Als Bitcoin im Januar 2009 anfing, wurden 50 Bitcoins pro Block »ausbezahlt«, im Jahr 2012 wurden es dann 25 Bitcoins und seit 2016 sind es 12,5 Bitcoins pro Block. Im Juni des Jahres 2020 wird die nächste Halbierung auf 6,25 Blöcke stattfinden

[20] Island, wo außerdem auch noch genügend kalte Luft zur Kühlung der Server vorhanden ist, ist der ideale Ort für das Schürfen von Bitcoin (siehe Ortlieb 2014, S. 1). Weil der Strom dort noch billiger ist, wird allerdings 80 Prozent aller Rechenleistung für Bitcoin in China zur Verfügung gestellt (Mayer-Kuckuk 2017, S. 15).

[21] Erfahrungsgemäß überholt die nächste Generation an Mining-Hardware jeweils aktuelle Geräte innerhalb weniger Monate und macht die alten Geräte dadurch zu Elektronikschrott (Schulz 2017a, S. 106).

(Hosp 2018, S. 91). Das Halving kann sich maximal 64 Mal ereignen, dann ist die kleinstmögliche Einheit – ein Satoshi – erreicht, die nicht weiter halbiert werden kann. Theoretisch wird der letzte Satoshi deshalb im Jahr 2040 ausgeschüttet (ebd., S. 92).[22] Weil außerdem die Energiekosten für Bitcoin-Blöcke ständig steigen, werden die Renditen beim »Mining« immer geringer. Die meiste Energie frisst der »Proof of Work«, mit dem die Erstellung eines neuen Blocks abgeschlossen wird. Er wird absichtlich so schwierig gestaltet, damit für ihn immer derselbe durchschnittliche Zeitraum benötigt wird. Diese Schwierigkeit wird auch als »Mining-Difficulty« (Mining-Schwierigkeit) bezeichnet. Der Bitcoin Algorithmus passt sich alle 2016 Blöcke (also etwa alle zwei Wochen) so an, dass das Gesamtnetzwerk etwa zehn Minuten benötigt, um einen Block zu erstellen (Hosp 2018, S. 74). Das soll gewährleisten, dass die Erstellung von Blocks immer eine gewisse Zeit benötigt, was die Blockchain besonders fälschungssicher macht. Dafür werden sogar extreme Energiekosten in Kauf genommen.

Mit dem Bitcoin sollten eigentlich drei Eigenschaften von Bargeld nachgeahmt werden: Anonymität, Unmittelbarkeit und das Fehlen von Transaktionskosten (Junge Linke 2012, S. 1). *Anonymität* ist bis heute weitgehend gegeben. Bei den Transaktionen wird lediglich die Bezeichnung der Bitcoin-Wallet registriert, nicht aber ihr Besitzer. Fraglich ist hingegen, ob man von *Unmittelbarkeit* sprechen kann. Ummittelbarkeit bedeutet, dass sich keine Instanz dazwischen schiebt – aber stellt die Bitcoin-Blockchain mit ihrem Netzwerk nicht selbst eine Instanz dar? Immerhin setzt sie ein riesiges technisches Aggregat voraus, das die Bitcoins überhaupt erst möglich macht und das für jede einzelne Transaktion – die mindestens zehn Minuten, aber auch bis zu einer Stunde in Anspruch nehmen kann – zwischen Nutzern in Bewegung gesetzt werden muss. Hinzu kommt noch – damit wären wir beim Thema *Transaktionskosten* –, dass die Transaktionen inzwischen in der Regel nicht mehr kostenfrei sind, wie noch

[22] Viele andere Kryptowährungen haben dagegen kein Halving oder ähnliche Reduzierungsmechanismen in ihrer Blockchain; sie haben also keine Mengenbegrenzung und sind damit tendenziell inflationär, während der Bitcoin tendenziell deflationär ist (Hosp 2018, S. 93).

in den Anfangszeiten der Bitcoins. Denn aufgrund der hohen Energie- und Rechnerkosten sind die Nutzer inzwischen dazu übergegangen, eine bestimmte Transaktionsgebühr zu bezahlen, damit ihr Auftrag überhaupt ausgeführt wird. Tatsächlich haben Bitcoin-Aufträge, die keine solche Gebühr anbieten, mittlerweile kaum noch eine Chance, ausgeführt zu werden, denn eine Überweisung gilt ja erst dann als getätigt, wenn sie aufgrund eines anerkannten Blocks erledigt wurde. Dabei können die Miner selbst auswählen, welche Aufträge sie in dem Block, den sie gerade erstellen, bearbeiten. Da in der Regel mehr Aufträge vorliegen als die erlaubten ca. 4200 Transaktionen pro Block, wählen sie diejenigen Transaktionen aus, die mit den höchsten Gebühren versehen sind (Hosp 2018, S. 68 f.). Wer dann einen erfolgreichen Block hergestellt hat, bekommt nicht nur die Mining-Belohnung, sondern erhält auch die Transaktions-Gebühren für die von ihm erledigten Aufgaben. Dieser Aspekt macht allerdings die Nutzung von Bitcoin als Bargeld zunehmend unattraktiv.

2.2 Erweiterung der Funktionen: Die Ethereum-Blockchain

Alle Kryptowährungen, bei denen es sich nicht um Bitcoins handelt, werden auch als »Altcoins« (»andere Coins«) bezeichnet. Diese schießen zur Zeit wie Unkraut aus dem Boden (Hosp 2018, S. 133). Momentan (Mitte 2018) gibt es, wie bereits erwähnt, etwa 1400 verschiedene von ihnen. Sie können auf drei verschiedene Weisen entstehen: Erstens als Abwandlung einer bestehenden Kryptowährung, wobei der Algorithmus der Blockchain mehr oder weniger stark modifiziert wird (aus der Bitcoin-Blockchain gingen zum Beispiel »Bitcoin Cash« und »Bitcoin Gold« hervor)[23]; zweitens als Neuschöpfung mit einer ganz eigenen Blockchain (wie etwa »Ethereum«); oder drittens als neue Kryptowährung, die jedoch auf einer anderen Plattform, (wie z.B. auf »Ethereum«) aufgebaut ist. Letzteres ist sogar die häufigste Variante.

[23] Vom Ursprung und dem ähnlichen Namen abgesehen, fungieren solche neuen Kryptowährungen vollkommen unabhängig auf ihrer jeweils eigenen Blockchain.

Nach dem Bitcoin ist die *Ethereum* die zweitbekannteste und -erfolgreichste Blockchain. Ihr erster Block wurde am 30. Juli 2015 generiert. Der Name ihrer Kryptowährung lautet »Ether«.[24] Anders als beim Bitcoin ist die Anzahl der Ether nicht begrenzt.[25] Wenn man Bitcoin als eine Blockchain der ersten Generation bezeichnet, dann ist Ethereum zweifellos eine Blockchain der zweiten Generation (Hosp 2018, S. 144). Sie ist eine der innovativsten Blockchains überhaupt, auf der ständig neue Anwendungsmöglichkeiten ausprobiert werden. Damit steht sie in starkem Kontrast zu Bitcoin, wo man eher auf die Vermeidung jeglicher Innovation setzt (ebd., S. 146). Dennoch – oder vielleicht gerade deswegen – genießt Ethereum eine ausgesprochen hohe Akzeptanz bei den Nutzern, und der Ether konnte sich neben dem Bitcoin als zweitbeliebteste Kryptowährung etablieren (ebd., S. 151). Anders als beim Bitcoin verwaltet die Ethereum-Blockchain nicht nur sich selbst (samt der eigenen Kryptowährung), sondern stellt die Grundlage für etliche weitere Anwendungen dar. Der grundlegende Gedanke ist der, dass Ethereum eine Art *»dezentralisierten Computer«* darstellen soll, auf dem Programme unaufhaltsam laufen (ebd., S. 145). Die Ethereum-Blockchain verfügt hierfür über ein Betriebssystem (die so genannte Ethereum Virtual Machine, kurz EVM).[26] Um ein Programm darauf laufen zu lassen, muss der Anwender des Programms dafür »Gas« (»Sprit«) bezahlen, und zwar in Ether.

Unter anderem ist das Ethereum-Betriebssystem auch dafür geeignet, andere Kryptowährungen auf ihm laufen zu lassen. Die Hauptfunktion der Ethereum-Blockchain ist aber die Speicherung und Bearbeitung von *Smart Contracts,* die hier erstmals zum Einsatz gekommen sind. Das sind Verträge, die in Code gegossen sind und sich quasi von selbst erfüllen (Schulz 2017a, S. 103). Auf diese Weise

[24] Auch hier gibt es eine kleinere Währungseinheit: Einem Ether entsprechen 1 Trillion »Wei« (das sind noch einmal zehn (!) Nullen mehr als beim Verhältnis von Bitcoin zu Satoshis).

[25] Auf der Ethereum Blockchain findet also kein Halving und auch sonst kein Reduzierungsmechanismus statt. Stattdessen ist die Mining-Belohnung immer die selbe.

[26] Um das EVM zu nutzen, muss man extra eine eigene Programmiersprache mit Namen »Solidity« lernen.

können verbindliche Vereinbarungen geschlossen werden, ohne dass Treuhänder, Mittelsmänner oder ähnliches erforderlich sind. Die Beteiligten eines solchen Vertrages müssen sich noch nicht einmal gegenseitig kennen. Ein einfaches Beispiel für einen Smart Contract wäre etwa ein Crowdfunding-Projekt. In solchen Projekten wird über das Internet eine bestimmte Menge Geld gesammelt; sobald eine vorher festgelegte Summe zusammengekommen ist, kann das Projekt (z.B. ein Film, der gedreht werden soll) gestartet werden. Was aber passiert, wenn die angestrebte Summe nicht zusammenkommt? Hier könnte ein Smart Contract aushelfen, der mit der folgenden Wenn-Dann-Funktion ausgestattet ist: Kommt die angestrebte Summe zusammen, dann wird sie an denjenigen überwiesen, der das Projekt durchführen will; passiert das jedoch bis zu einem bestimmten Zeitpunkt nicht, dann wird das Geld an die Investoren zurücküberwiesen. So kann man sich mit Hilfe eines Smart Contracts das Honorar für einen Treuhänder sparen (siehe Schulz 2017b, S. 23). Einige Unternehmen zeigen zwar ein gewisses Interesse an Smart Contracts, allerdings gilt dieses Verfahren derzeit noch als zu schwerfällig und zu energieintensiv (Schulz 2017a, S. 106).

2.3 Risiken und Nebenwirkungen

Sämtliche Kryptowährungen haben das Problem, dass sie aufgrund der Schwerfälligkeit der Zahlungsvorgänge sowie ihrer hohen Wertschwankungen kaum als alltagstaugliches Zahlungsmittel geeignet sind. Von einem Wert von Null bis zu 20.000 Dollar hatte der Bitcoin bisher alle Werte inne, darunter befanden sich auch drastische Kursstürze.[27] Infolge seiner starken Volatilität werden die

[27] Grob nachgezeichnet nahm der »Wert« des Bitcoin folgenden Verlauf: 2009, dem Jahr seiner Erstausgabe, hatte er überhaupt noch keinen Marktpreis. Nach etwa einem Jahr bekam man einen Cent pro Bitcoin, und im Jahr 2011 erreichte er dann erstmals den Wert von einem US-Dollar (siehe Hosp 2018, S. 138 u. 141). Danach ging es zunächst eher moderat weiter, bis er im Lauf des Jahres 2013 plötzlich auf fast 1000 US-Dollar stieg. Ein Jahr später platzte die erste Bitcoin-Blase. 2014 und 2015 fiel er von rund 1000 US-Dollar auf 200 Dollar (ebd., S. 23), weil die seinerzeit wichtigste Bitcoin-Börse MtGox gehackt und die Guthaben etlicher Bitcoin-Besitzer geplündert wurden. Dennoch begann der Bitcoin gegen Ende 2015 allmählich wieder zu steigen. Besonders

allermeisten Bitcoins nicht für Käufe als Zahlungsmittel, sondern wird vor allem zur »Währungsspekulation« (Ortlieb 2014, S. 4) eingesetzt. Um als Geld im täglichen Zahlungsverkehr zu dienen, müsste dieser stabil sein. Davon ist er meilenweit entfernt.

Sofern Kryptowährungen überhaupt als Zahlungsmittel eingesetzt werden, dienen sie vorwiegend für Transaktionen innerhalb der Schattenwirtschaft (siehe Landgraf 2018, S. 3). Dort werden sie für den illegalen Handel z.B. mit Drogen oder Waffen eingesetzt.[28] Des öfteren werden auch Vermögen an der staatlichen Kontrolle vorbei ins Ausland transferiert (Hickel 2017, S. 12). Besonders übel ist ihr Einsatz im Menschenhandel oder bei Erpressungen. Bei letzteren war bisher die Geldübergabe der kritischste Moment, in dem die meisten Täter gefasst werden konnten. Mithilfe von Bitcoin und Co. kann dieser wunde Punkt relativ leicht umgangen werden, und daher kommt es immer häufiger vor, dass Lösegeldzahlungen in Form von Kryptowährungen verlangt werden.

Eine weitere Problematik der Blockchain-Technologie und damit auch der Kryptowährungen ist der extrem hohe Energiebedarf. Der Grund dafür liegt vor allem im »Proof of Work«. Wie oben beschrieben, muss die entsprechende Berechnung für jeden einzelnen Block enorm oft vollzogen werden, nämlich so lange, bis eine Zahlenkombination herauskommt, die das verlangte Kriterium erfüllt. Bis dahin werden unzählige Berechnungen angestellt, die sich als ungültig herausstellen (Schulz 2017a, S. 105). Dabei rechnen innerhalb eines Blockchain-Netzwerks enorm viele Computer gleichzeitig um die Wette. Sie alle verbrauchen riesige Mengen an Rechenzeit und Energie für das Lösen von

rasant wurde es 2017: Im März 2017 wurde die bisherige Obergrenze von 1000-Dollar geknackt, im Mai die 2000-Dollar-Marke genommen (Kaufmann 2017a, S. 16). Im Oktober 2017 wurde dann die 6000 Dollar-Grenze überschritten, Anfang November 2017 die 7000 Dollar-Grenze und Ende November sogar die 10.000-Dollar-Marke; Mitte Dezember 2017 befand sich der Bitcoin dann auf einem Rekordhoch von 20.000 Dollar. Seitdem ging es fast nur noch abwärts, bis er Anfang Februar 2018 unter 6000 Dollar rutschte und dort lange verharrte. Zurzeit (Mitte 2018) schwankt er zwischen 5000 und 7000 Dollar.

[28] Für den Handel mit Cannabisprodukten wurde extra der »Potcoin« eingeführt, um damit anonym Marihuana und Co. zu bezahlen (Klein 2018, S. 2.).

Aufgaben, wobei aber nur ein einziger davon als »Gewinner« wirklich einen neuen Block herstellt. Noch ein weiteres Mal vervielfacht sich der überflüssige Energieverbrauch durch das laufende Entstehen von Verzweigungen (Forks), bei denen hoher Energieaufwand in Blöcke eingeht, die ohnehin verworfen werden.

Der gesamte dabei anfallende Energieverbrauch dient einzig und allein dem Zweck, die betreffende Blockchain *öffentlich und zugleich fälschungssicher* zu machen. Wegen des Wettrennens ist es außerdem für alle beteiligten Miner enorm wichtig, über die neueste leistungsfähige Hardware zu verfügen, weil sie sonst überhaupt keine Chance haben. Aus den genannten Gründen verursacht allein die Bitcoin-Blockchain derzeit ein Promill des weltweiten Energieverbrauchs (Voß 2018, S. 2). Das ist mehr Strom, als ein mittelgroßer Staat – wie zum Beispiel Irland oder Marokko – benötigt (Wille 2017, S. 16). Wäre es ein Staat, läge das Bitcoin-System auf Platz 61 des internationalen Energiebedarfs. Und seine Verbrauchskurve weist weiter steil nach oben. Verläuft sie weiter so wie bisher, dann wird der Bitcoin bereits im Jahr 2019 mit dem Niveau der USA den Spitzenplatz auf der Tabelle erreichen (ebd.). Blockchains sind daher aus ökologischer Sicht eine Katastrophe.

3. Sind Kryptowährungen eigentlich Geld?

3.1 Was macht Geld zu Geld?

In der kapitalistisch verfassten Gesellschaft ist Geld der Repräsentant des abstrakten gesellschaftlichen Reichtums, und seine Vermehrung ist Zweck bzw. Selbstzweck der Produktion. Dass seine begriffliche Bestimmung in den führenden Wirtschaftstheorien dennoch unterbelichtet bleibt, verweist auf deren Blindheit gegenüber der kapitalistischen Form.[29] Münzen, Banknoten, Buchungen, Kontenverzeichnisse etc. *symbolisieren* nach deren Auffassung lediglich Wert und seien wesensverschieden von den Waren. Geld stellt nach dieser Lesart lediglich eine zwischen den Gütermarktwaren vermittelnde Instanz, ein Mittel, dar, das dazu dient, den Güteraustausch zu erleichtern, selbst jedoch keinen Wert besitzt und daher nur ein substanzloses Zeichen ist.

Schon ein simpler Blick in die Geschichte des Geldes dementiert dies jedoch. Das erste Geld bestand aus Gold, Silber und teilweise auch anderen (mehr oder weniger) edlen Metallen bzw. Legierungen (wie beispielsweise Kupfer oder Bronze) und konnte seine Funktion nur erfüllen, weil es einen gesellschaftlich anerkannten Wert repräsentierte und sich daher der Wert der anderen Waren in ihm darstellen ließ.[30] Rein logisch hätte im Grunde jede Ware zum Geld werden

29 Wie Arne Heise, seines Zeichens selbst Ökonom und Direktor des Zentrums für Ökonomische und Soziologische Studien an der Universität Hamburg, feststellt, ist der Zustand der Wirtschaftswissenschaften ohnehin kritisch. Besonders »die herrschende Lehre – der neoklassische Mainstream – ähnelt in seiner dogmatischen Einseitigkeit eher einer Glaubenslehre als einer wissenschaftlichen Disziplin. Ihr muss man sich unterwerfen oder man wird als Wissenschaftler nicht ernst genommen« (Heise 2018, S. 10).

30 Julian Hosp versteigt sich allerdings in die Behauptung: »Sogar »Gold hat KEINEN inhärenten Wert« (Hosp 2018, S. 33, Großschreibung im Original). Dabei verkennt er jedoch, dass das Auffinden, Zutage-Fördern und Bearbeiten von Gold bestimmte Mengen an gesellschaftlich notwendiger durchschnittlicher Arbeitszeit erfordert, was ihm einen Eigenwert verschafft. Zumal es für Gold bestimmte Anwendungen (z.B. als Zahn- oder Industriegold sowie in der Schmuckherstellung) gibt, was ihm auch einen sinnlich-stofflichen Gebrauchswert verschafft. Beides macht das Gold zu einer vollwertigen und damit werthaltigen Ware wie alle anderen Waren auch. Andere

können. Metalle und vor allem Edelmetalle haben aber bestimmte, äußerst praktische Eigenschaften, die schon der griechische Philosoph Aristoteles zu schätzen wusste: Sie sind enorm haltbar, leicht transportierbar (und somit auch leicht zwischen den Menschen übertragbar) sowie, nicht zuletzt, gut teilbar. All das sind Eigenschaften, die sie besonders gut als Geld qualifizieren.

Nun hatte Geld in der Antike und in vormodernen Zeiten eine ganz andere gesellschaftliche Bedeutung und Stellung als heute. Erst in der kapitalistischen Gesellschaft kann man mit Marx davon sprechen, dass das Geld den Charakter einer »allgemeinen Ware« einnimmt, die zur Darstellungsform des Tauschwerts aller anderen besonderen Waren wird und die zugleich den abstrakten Reichtum der Gesellschaft, den Wert, repräsentiert. Voraussetzung für die Aussonderung dieser allgemeinen Ware aus dem Universum der besonderen Waren ist allerdings, dass sie selbst einen Wert darstellt, der sich auf die abstrakte Arbeit zurückführen lässt (vgl. Marx 1988, S. 532 und Lohoff 2018). Dass Gold letztlich diese Stellung einnahm (nach einer gewissen Übergangszeit des Bimetallismus von Gold *und* Silber) hat historische Gründe, was aber nicht zu der Annahme verleiten sollte, das Wesen des Geldes in der kapitalistischen Gesellschaft ließe sich einfach aus seinem geschichtlichen Werdegang bestimmen. Der Kapitalismus entsteht zwar nicht im luftleeren Raum, unterzieht jedoch die vorgefundenen gesellschaftlichen Bedingungen und Kategorien einem grundlegenden Formwandel. Dennoch können aus der Geschichte des Geldes einige Erkenntnisse gewonnen werden, wenn wir die Unterschiede zwischen Vormoderne und kapitalistischer Moderne im Auge behalten.

Betrachten wir zunächst die Goldmünzen, die es seit der Antike gibt, die aber noch bis weit ins 19. Jahrhundert und zum Teil bis ins 20.Jahrhundert zirkulierten. Interessant an der Münze ist, dass sie zwei wesentliche Momente des Geldes gleichzeitig in sich trägt, die im Verlauf der Geschichte voneinander

Kryptoexperten sind schon weiter. So kann man etwa in den Allgemeinen Geschäftsbedingungen (AGB) der wichtigsten deutschen Bitcoin-Börse »Bitcoin Deutschland AG« lesen: »Anders als etwa Münzgeld kommt einem Bitcoin auch kein vom Tauschwert losgelöster Gebrauchswert zu« (Bitcoin Deutschland AG, § 9, Abs. 1).

geschieden werden sollten. Durch die einheitliche Form und den Prägestempel wird eine Münze nämlich *einerseits* zum *Geldzeichen, zugleich* ist sie aber auch aufgrund ihres eigenen Edelmetallgehalts *unmittelbarer Träger von Wert.* »In der Münze fällt damit die gesellschaftliche Formbestimmtheit des Geldes (als ausgesondertes Zirkulationsmittel) ganz mit seiner Materialität zusammen« (Müller 1981, S. 67).[31] In diesem ersten Auftritt als Geldzeichen liegt ein Grund für die falsche Auffassung des Geldes als eines *bloßen* Zeichens, die in der nominalistischen Geldtheorie (und damit bei praktisch allen bürgerlichen Ökonomen)[32] als einzige anerkannt ist (ebd., S. 59).

In Form der Münze sind Geldzeichen und werthaltige Geldware noch miteinander vereint. Es ist aber möglich, beide voneinander zu trennen. Das war historisch zum Beispiel der Fall bei Wechseln, die privat ausgestellt wurden und jeweils eine bestimmte Geld- (sprich Gold- oder Silber-)Menge repräsentierten. Jeder Wechsel konnte beim Aussteller oder auch bei anderen explizit im Wechsel genannten Personen wieder gegen Gold eingetauscht werden. Die ersten beurkundeten Wechsel wurden zu Begin des 13. Jahrhunderts in Norditalien ausgestellt. Endgültig etabliert hatte sich ihre Verwendung gegen Ende des 16. Jahrhunderts. Unter anderem spielten sie damals eine wichtige Rolle für die Handelsachse Norditalien-Niederlande.[33] In diesen beiden Regionen lagen im 16. Jahrhundert die bedeutendsten Handelsstädte des Abendlandes, zwischen denen seinerzeit ein reger Austausch stattfand. Dabei erwies es sich als äußerst unpraktisch, ständig große Goldmengen über die Alpen hin und her zu transportieren. Stattdessen wurden Wechsel über das Gold ausgestellt, auf deren

[31] »Münzen können zwar gestempelt usw. sein – sie fungieren als Zirkulationsmittel aber wesentlich aufgrund ihres jederzeit überprüfbaren Metallgewichts und -feinheitsgrades« (Müller 1981, S. 58).

[32] Einschließlich der Keynesianer. Bereits Adam Smith war der Auffassung, dass Geld und Ware wesensverschieden seien, wobei er den Wertgehalt der Münze (sprich: die Tatsache, dass sie aus einem werthaltigen Metall bestand) offensichtlich ignorierte. Nicht zuletzt gibt es selbst Anhänger der Marx‘schen Theorie, die der nominalistischen Geldtheorie anhängen, beispielsweise Michael Heinrich.

[33] Zu den Niederlanden zählte damals noch Flandern.

Grundlage die Ansprüche auf entsprechende Gold- oder Silbermengen dann in den jeweiligen Heimatstädten diskontiert (miteinander verrechnet) werden konnten, während das eigentliche Edelmetall unbewegt und sicher in seinen Depots blieb. Da Wechsel als Zeichen für bestimmte Edelmetallmengen standen und der Handel mit ihnen offenbar gut funktionierte, bürgerte es sich schließlich ein, Wechsel auch zum Bezahlen an Dritte einzusetzen. Damit fungierten sie ähnlich wie Geld – sie stellten gewissermaßen privat erzeugte Geldsurrogate dar, die real vorhandenes Geld (Gold oder Silber, das an anderer Stelle sicher gelagert war) repräsentierten. Historisch folgten den privaten Wechseln schließlich die Banken, die standardisierte Papiernoten ausstellten, die ebenfalls Gold (oder Silber) repräsentierten, das in den betreffenden Banken eingelagert war. Wechsel und die Banknoten der Privatbanken leiteten die reale Scheidung von Geld*zeichen* einerseits und Geld*ware* andererseits ein, stellten aber noch keine allgemein anerkannten Geldzeichen dar. Bei ihnen handelte es sich noch um private Geldsurrogate, die auf einen bestimmten Kreis von Personen bzw. Institutionen beschränkt waren. Diese Geldsurrogate nahmen eine Stellvertreterfunktion für die Geldware ein, was seinerzeit leicht daran zu erkennen war, dass man sie bei den entsprechenden Handelspartnern bzw. Banken gegen die echte Geldware (sprich: die entsprechende Gold- oder Silbermenge) eintauschen konnte. Später ging das Recht, Banknoten auszugeben, exklusiv auf die Zentralbanken über. Mit diesem Papiergeldmonopol der Zentralbanken war zugleich der Wechsel vom privaten Geldderivat zum allgemein anerkannten Zahlungsmittel und damit zum *Geldzeichen* vollendet. Jetzt waren Geldzeichen und Geldware eindeutig und allgemeinverbindlich voneinander geschieden, und es wurde schließlich für jedermann ganz selbstverständlich, Banknoten als Zahlungsmittel zu verwenden.

Seitdem hat die Geldware tiefgreifende Umwälzungsprozesse durchgemacht. Zunächst waren die Zentralbanken noch dazu verpflichtet, für die ausgegebenen Geldzeichen eine entsprechende Menge an Gold zu bevorraten. Dabei wurde die Einlagerungspflicht von Gold jedoch allmählich aufgeweicht: »Die Bank von England beispielsweise war verpflichtet, zwei Drittel der umlaufenden Banknoten mit Gold zu decken. Für das übrige Drittel war ihr gestattet, erstklassige

Handelswechsel zu halten, was mit Zinseinnahmen verbunden war« (Born 1977, S. 24). Dennoch war Gold bis zum Jahr 1914 weltweit die eigentliche Geldware. Das hatte unter anderem den Vorzug, dass Pfund, Dollar, Franc, Mark etc. damals ohne große Probleme untereinander getauscht werden konnten, da jede Einheit einer Währung an eine definierte Menge Gold gekoppelt war, was sie sehr leicht miteinander vergleichbar machte.

Allerdings ließ sich die Golddeckung auf Dauer nicht halten; denn die Produktion an Waren schwoll im Zuge der fortschreitenden Kapitalakkumulation derart an, dass sie mit dieser nicht mehr kompatibel war. Das hat einen logischen Grund: Eine aufgrund natürlicher Bedingungen in ihrer Menge begrenzte Geldware ist auf Dauer nicht funktional für eine Produktionsweise, in der das Geld den abstrakten Reichtum repräsentiert, der als Selbstzweck der Produktion permanent vermehrt werden muss. Das zeigte sich praktisch bereits zu Beginn des 20. Jahrhunderts darin, dass Gold in Mengen benötigt wurde, die einfach nicht vorhanden waren, und es deshalb allmählich zu einer Aufweichung der Golddeckung kam. In Deutschland genügte es im Jahr 1909 beispielsweise, wenn 40 Prozent der im Umlauf befindlichen Münzen und Banknoten durch Gold gedeckt waren. So verlor das Gold allmählich seine Funktion als Geldware, bis diese dann mit dem Beginn des Ersten Weltkriegs schlagartig annulliert wurde, als in vielen Ländern angesichts der horrenden Kriegskosten die Goldeinlösepflicht der Notenbanken ausgesetzt werden musste. Bereits im August 1914 (dem Monat des Kriegsausbruchs) schafften Deutschland, Frankreich und Russland die Golddeckung ihrer jeweiligen Währung ab, Großbritannien folgte wenig später. Unter dem strengen Regime einer Goldwährung ließen sich die auflaufenden Kriegskosten einfach nicht mehr finanzieren.[34] Gut 30 Jahre später, nach dem Ende des Zweiten Weltkriegs, wurde die Goldbindung in den westeuropäischen Ländern dann zwar noch einmal eingeführt, allerdings nur indirekt. Das System

[34] Auch nach dem Ersten Weltkrieg wurde die Golddeckung in den betreffenden Ländern nicht wieder eingeführt. Sie hätte die Behebung der Kriegsschäden enorm behindert. Im Fall Deutschlands kamen außerdem noch die Reparationspflichten hinzu, die mit einer goldgedeckten Währung erst recht nicht zu stemmen gewesen wären.

von Bretton-Woods koppelte die westeuropäischen Währungen in einem festen Wechselkursverhältnis – das gelegentlich leicht nachjustiert werden musste – an den Dollar, der bis dahin seine Golddeckung noch nie verloren hatte.[35] Damit sollten die Wirtschaftsbeziehungen innerhalb des westlichen Blocks stabilisiert und gefestigt werden.

Kriegsbedingt hatte die USA nach dem Zweiten Weltkrieg zunächst einen enormen ökonomischen Vorsprung gegenüber allen anderen westlichen Ländern. Das System der festen Wechselkurse wurde daher großzügig zugunsten der Europäer zugeschnitten, die sich rasch vom Krieg erholen sollten, um als Bollwerk gegenüber der als Bedrohung gesehenen Sowjetunion zu fungieren.[36] In dem Maße, in dem die Westeuropäer ihre Industrien wieder aufbauten, schmolz der Vorsprung der USA allerdings dahin, was diesen wiederum zunehmende wirtschaftliche Probleme bereitete. Hinzu kamen seit den 1960er-Jahren die explodierenden Kosten des Vietnamkrieges. Beides führte dazu, dass die USA ihre goldgestützte Währung schließlich ihrerseits nicht mehr aufrechterhalten konnten. Mit der Aufhebung der Goldkonvertibilität des US-Dollar im Jahr 1971 schlug dann konsequenterweise auch die Stunde des Systems der festen Wechselkurse unter den westlichen Währungen. Damit hatte das Gold als Geldware endgültig ausgedient (siehe auch Lohoff 2018).[37] Das Gros der Ökonomen zog aus dieser Tatsache das Fazit, dass es seitdem überhaupt keine Geldware mehr gibt und die Geldzeichen heutzutage völlig ungedeckt zirkulieren. Hierbei handelt es sich jedoch um einen Fehlschluss; vielmehr verhält es sich so, dass seitdem die Zentralbanken eine ganz andere Art von Geldware vorhalten, auf

[35] Nach innen hatten die USA allerdings die Goldkonvertibilität seit 1933 aufgehoben. Damals hatte die Roosevelt-Regierung im Rahmen des New Deal den US-Bürgern privaten Goldbesitz untersagt. Dieses Verbot fiel erst im Jahr 1971, als auch die allgemeine Aufhebung der Goldbindung des US-Dollars endete (Lohoff 2018).

[36] Einige Ökonomen, beipielsweise Heiner Flassbeck und Friederieke Spiecker (2007), sind der Auffassung, dass das System von Bretton Woods stärker zum Wiedererstarken der deutschen (sowie generell der westeuropäischen) Wirtschaft beigetragen hat als der Marshall-Plan.

[37] Als letzte Währung der Welt verlor schließlich der Schweizer Franken am 27. Mai 1998 seine Goldbindung.

die sich die zirkulierenden Geldzeichen beziehen. Auch dieser Prozess verlief schrittweise, wobei die neue Geldware das Gold sukzessive ablöste.

3.2 Die neue Geldware in der Ära des fiktiven Kapitals

Wie bereits erwähnt, lagerte schon die Bank von England im 19. Jahrhundert nicht nur Gold, sondern auch hochkarätige Handelswechsel zur Deckung der von ihr ausgegebenen Banknoten in den Tresoren. Nun stellen aber auch Handelswechsel – genauso wie andere Wertpapiere – eine Art von Ware dar. Allerdings handelt es sich hierbei nicht um *Güter*marktwaren, sondern um *Finanz*marktwaren. Mit dem Wegfall der Goldbindung kam es daher nicht zum Verschwinden jeglicher Geldware, sondern zu einer Umstellung von der Deckung durch eine Gütermarktware (dem Gold) zu einer Deckung durch Finanztitel[38], die ihrerseits Bestandteil eines *Finanzwarenmarktes* sind. Nun ist nach der Auffassung von Ernst Lohoff (2018), der ich mich im Folgenden anschließe, auch der Finanzwarenmarkt ein Warenmarkt, der sich auf die Schöpfung von Wert bezieht. Finanzmarktwaren weisen allerdings die Besonderheit auf, dass sie keinen bereits geschaffenen Wert darstellen (wie das bei jeder Gütermarktware der Fall ist), sondern vielmehr auf der Erwartung von künftig erst zu schaffendem Wert beruhen: »Die verschiedenen Eigentumstitel, die die Zentralbanken im Rahmen ihrer Geldschöpfung akkumulieren, haben nun einmal im Gegensatz zur klassischen Geldware Gold keinerlei sinnlich-stofflichen Gebrauchswert, sondern nur den übersinnlichen Gebrauchswert, künftige Wertproduktion zu repräsentieren« (Lohoff 2018). Bei den Waren der Finanzmärkte handelt es sich um Wertpapiere, z.B. um verbriefte Kredite oder um Aktien (um nur die gängigsten Wertpapiere zu nennen). Deren Wert begründet sich in der Zukunft: Beim Konsumentenkredit wird erwartet, dass der Kreditnehmer den entsprechenden Gegenwert durch künftige eigene Arbeitsverrichtung schafft, Investitionskredite gehen von einer entsprechenden Wertschöpfung durch die Produktion im kreditnehmenden Un-

[38] Die Begriffe »Finanztitel«, »Finanzmarktware«, »Eigentumstitel« und »Wertpapier« verwende ich im Folgenden synonym.

ternehmen aus, und Aktien antizipieren die künftige Wertschöpfung innerhalb der betreffenden Aktiengesellschaft. Während also die Gütermarktwaren Wert darstellen, weil für ihre Produktion in der *Vergangenheit* Arbeitskraft verausgabt wurde, ist bei den Finanzmarktwaren der Zeitpfeil umgedreht: Der Wert, den sie repräsentieren, soll erst in der *Zukunft* geschöpft werden. Dieser zukünftige Wert kann allerdings in der Gegenwart bereits kapitalisiert werden, eine Besonderheit, die es erlaubt, Kapital zu akkumulieren, ohne Wert zu verwerten (Lohoff u. Trenkle 2012, S. 124 ff.; Lohoff 2014). Um den besonderen Charakter dieser Form von Kapital hervorzuheben, bezeichnet man es als »fiktives Kapital«.[39]

Da nun aber das fiktive Kapital schon seit den 1980er-Jahren zum Dreh- und Angelpunkt der Kapitalakkumulation geworden ist, kann es eigentlich nicht verwundern, dass zeitgleich damit auch die Finanztitel, die sich im Besitz der Zentralbanken befinden, die Position der Geldware eingenommen haben. Dass diese tatsächlich als neue Geldware fungieren, ist schon daran zu erkennen, dass die Notenbanken neues Geld nicht einfach in einer Weise unter die Leute bringen, wie der Weihnachtsmann Geschenke verteilt, sondern dafür einen Gegenwert in Gestalt eben solcher Wertpapiere verlangen. Praktisch gelangt das sogenannte Zentralbankgeld durch Kreditvergabe sowie durch den Ankauf von Wertpapieren durch die Zentralbank in Umlauf; selbst die Einspeisung des Bargelds in den Wirtschaftskreislauf erfolgt auf diesem Wege (siehe Lohoff 2018). Für jeden Geldbetrag[40], den die Zentralbank in die Welt setzt, nimmt sie entsprechende Wertpapiere entgegen, die sie in ihren Tresoren einlagert. Indem sie Papiere ankauft und dabei zugleich neue Geldzeichen herausgibt, macht die Zentralbank die betreffenden Papiere zugleich zur Geldware. Anders als beim per se einheitlichen Gold setzt sich der Bestand der Geldware aus sehr vielen *verschiedenen* Wertpapieren zusammen, deren Zusammensetzung sich außerdem laufend ändert, nämlich mit jeder Herausgabe neuer Geldzeichen und

[39] Der Begriff »fiktives Kapital« wurde von Karl Marx im dritten Band des »Kapital« geprägt (siehe Marx 1988, S. 413 ff.).

[40] Das sind übrigens größtenteils Geldbuchungen; nur ein relativ kleiner Teil des Zentralbankgeldes wird in Form von Banknoten und Münzen herausgegeben.

dem damit verbundenen Ankauf neuer Wertpapiere. Jedes in der Zentralbank eingelagerte Wertpapier wird damit automatisch zur Geldware, während es diese Eigenschaft sofort wieder verliert, wenn es die Tresore bzw. Bilanzen der Zentralbank verlässt.

Generell gilt, dass das Geldsystem nur so lange stabil bleibt, wie es durch den Wert einer Geldware abgesichert ist. Gold war in dieser Hinsicht besonders sicher, denn als Gütermarktware fußte es auf vergangener Wertproduktion. Ferner kann seine Produktion nicht beliebig erhöht werden, wodurch es weitgehend entwertungsresistent war; allerdings war es, wie schon dargelegt, genau aufgrund dieser Limitierung für eine ständig fortschreitende Kapitalakkumulation auf Dauer nicht geeignet. Deshalb liegt seine Ablösung durch eine neue, unbegrenzt vermehrbare Geldware in der inneren Logik der kapitalistischen Produktionsweise mit ihrer versachlichten historischen Dynamik begründet. Allerdings stellt die neue Geldware keinesfalls eine längerfristig stabile Grundlage für das Geldsystem dar; denn die Eigentumstitel fußen auf künftiger Wertproduktion, die auch scheitern kann und im Zuge des weiter fortschreitenden Krisenprozesses auch im großen Stil scheitern wird (vgl. Lohoff 2018). Doch gerade das dann unvermeidliche Übergreifen der Krise auf das Geldsystem selbst wird noch einmal den negativen Beweis dafür liefern, dass dieses ohne eine Geldware nicht funktionieren kann.

Dieser Umstand, dass auch heute noch den im Umlauf befindlichen Geldzeichen eine entsprechende Menge an Geldware in Form von in der Zentralbank eingelagerten Wertpapieren gegenüber steht, wird von den etablierten Ökonomen notorisch übersehen. Damit wird aber die Geldware, die für die Deckung der zirkulierenden Geldzeichen sorgt, systematisch ausgeblendet. Das spiegelt sich auch im fragwürdigen Begriff der »*Geldschöpfung*« wider. Dieser legt nahe, dass die Notenbanken vollkommen willkürlich neues Geld in Umlauf bringen könnten. Faktisch gehören aber hier, wie bei jeder anderen Kreditbeziehung auch, immer zwei dazu, nämlich der Leiher und der Verleiher. Das sollte sich eigentlich von selbst verstehen. Dagegen suggeriert der Begriff »Geldschöpfung« einen einseitigen Akt mit der Zentralbank als Schöpfergott (ebd.) – ein

grundlegender Denkfehler, dem praktisch alle heutigen Ökonomen erliegen. Dasselbe gilt übrigens für den Ausdruck »Fiatgeld« (lat.: »Es werde Geld!«), der als Fachausdruck daherkommt, aber faktisch die gleiche Verwirrung stiftet wie der Begriff der »Geldschöpfung«. Beide unterstreichen die falsche Auffassung, wonach heutigen Banknoten keine Geldware mehr gegenüber stehe, weil das Zentralbankgeld angeblich das Ergebnis einer einseitigen Setzung durch die Zentralbanken sei. In Wirklichkeit entspringt alles Geld jedoch immer einem Interaktionsverhältnis. Die Zentralbanken können nur Geld »schöpfen«, indem sie mit Geschäftsbanken in eine Kreditbeziehung treten (ebd.), was diese wiederum in der Regel nur tun, wenn sie geeignete Kreditnehmer finden, die eine künftige Wertschöpfung (sprich: die Produktion von Gütermarktwaren) in Aussicht stellen.[41] Auf der heutigen Entwicklungsstufe des Kapitalismus hat das gesamte Geldsystem somit zwar nahezu ausschließlich die *Wertantizipation* zum Inhalt, aber es gibt nach wie vor einen inneren Zusammenhang zwischen Wert, Ware und Geld. Anders gesagt: *Es kann kein Geld ohne Geldware geben.* Vor dem Hintergrund dieser Erkenntnis soll nun der Frage nachgegangen werden, ob Bitcoin und Co. angesichts der bisherigen Begriffsklärungen überhaupt Geld darstellen können.

3.3 Bitcoins: (Kein) Geld der Krise

Kryptowährungen kommen ohne Banken, ohne Staat (und damit auch ohne Zentralbanken) sowie ohne jede sonstige zentrale Organisationsform aus. Geschaffen werden sie einzig und allein durch Privatleute bzw. -unternehmen mit ihren Computern, die sie mit entsprechenden Programmen in Gang halten. Dabei entstehen die Kryptocoins aus dem Nichts. Anders als bei den herkömmlichen Geldzeichen steht ihnen keinerlei Geldware gegenüber; nirgendwo ist irgend etwas gelagert, das einen Wert repräsentiert, auf den sie verweisen könn-

[41] Dabei handelt es sich nicht selten um sehr lange finanzielle Ketten, deren einzelne Glieder aus Krediten oder anderen Wertpapieren bestehen. Das tut der Tatsache keinen Abbruch, dass am Ende immer das Versprechen auf die Herstellung von Gütermarktwaren steht, die einen Wert repräsentieren.

ten. Das ist ein ganz wesentlicher Unterschied zum Notenbankgeld. Dieses hat, wie gezeigt, auch heute noch durch die bei der Zentralbank eingelagerten Wertpapiere immer einen Bezug zur Wertschöpfung, mag dieser Bezug auch noch so indirekt sein, noch so sehr auf die Zukunft verweisen und über noch so viele Zwischenglieder verfügen.

Bitcoin und Co. haben nichts dergleichen. Sie sind durch keinerlei Wert gedeckt, nicht einmal durch einen erst zukünftig zu schaffenden Wert.[42] Anders als alles andere, was bisher als Geld bezeichnet wurde, basiert der »Wert« von Kryptogeld allein auf dem Glauben aller Beteiligten (Landgraf 2018, S. 2); er entsteht allein dadurch, dass Menschen bereit sind, sie zu kaufen. Der Preis ihrer jeweiligen Coins bildet sich einzig und allein aufgrund der Erwartung, dass es immer noch jemand anderen geben wird, der bereit ist, noch mehr Geld (in allgemein anerkannten Währungen) dafür zu geben, als man selbst dafür gezahlt hat. Insofern weisen Bitcoin und Co. eher die Merkmale eines typischen Spekulationsobjekts als die von Geld auf.

Nun stellen zwar die Anhänger der Kryptowährungen selbst immer gerne die Analogie zum Gold her, um sich und anderen zu suggerieren, dass es sich um ein stabiles Geld handle. Dazu gehört bei den Bitcoins etwa die technisch gewollte Knappheit, und auch der Begriff des »Mining« verweist darauf. Aber schon auf den ersten Blick sticht ein gravierender Unterschied zum Gold ins Auge. Eine Kryptowährung kann nämlich nur so lange vorhanden sein, wie die Blockchain existiert, auf der sie beruht. Anders als Gold existieren Bitcoin und Co. nicht einfach weiter, sobald sie einmal »geschürft« wurden. Sowohl ihr weiteres Vorhandensein wie auch ihr Händewechsel sind zwingend auf den Betrieb der betreffenden Blockchain und damit auf eine komplexe Technologie samt umfangreicher digitaler Infrastruktur angewiesen. Damit nicht genug, steigen die Kosten für diese unverzichtbaren Voraussetzungen unaufhörlich an.

[42] Auch die Tatsache, dass der Bitcoin limitiert ist, indem seine Menge verbindlich auf 21 Millionen Exemplare festgelegt ist, verschafft ihm noch keinen Wert. Hier liegt der Fehlschluss vor, dass ein Zahlungsmittel seinen Wert angeblich seiner Knappheit verdankt.

Der einzige Grund, diese Kosten zu bestreiten, um die Blockchain weiter in Gang und damit das Kryptogeld am Leben zu halten, liegt in der Belohnung in Form des Kryptogeldes selbst. Daher muss der Marktpreis der betreffenden Kryptowährung stets hoch genug sein, um die laufenden Mining-Kosten zu ersetzen und außerdem einen gewissen Profit zu ermöglichen, denn letztlich sind Miner nicht anderes als Unternehmen, deren Investitionen sich rentieren müssen. Es handelt sich um akkumulierende Einzelkapitale, und als solche stellen sie ihre Tätigkeit in dem Moment ein, in dem sie keine Profite mehr erwirtschaften können. Damit schwebt über jeder Kryptowährung die ständige Gefahr, dass ihre Blockchain in dem Moment zu funktionieren aufhört, in dem ihr Marktpreis zu tief fällt, um die eigenen Mining-Kosten zu decken.[43] Anders ausgedrückt: Kryptowährungen sind praktisch jederzeit von der Gefahr ihres eigenen Verschwindens bedroht. Es liegt daher auf der Hand, dass sie unter diesen Umständen auch die wichtigen Geldfunktionen der Wertaufbewahrung und des Wertmaßstabs nicht erfüllen können und daher auch für den ganz normalen Zahlungsverkehr kaum geeignet sind. Genau betrachtet, bleibt dann aber kaum noch etwas übrig von dem Selbstverständnis der Kryptowährungen. Es handelt sich im Grunde um ein aufwendig produziertes Spekulationsgut, nicht aber um Geld.

Dass Kryptowährungen dennoch ernsthaft als mögliche Alternative zum Zentralbankgeld diskutiert und behandelt werden, sagt vor allem einiges über den schlechten Zustand der Notenbanken und des von ihnen ausgegebenen Geldes aus. Das geldpolitische Instrumentarium ist durch die Finanzkrise von 2008 und deren vorübergehende Bewältigung schwer in Mitleidenschaft gezogen worden. Das gilt zum einen für den Leitzins, dem wichtigsten Instrument zur Steuerung der Geldmenge: Je höher die Zinsen, umso unattraktiver ist es, sich Zentralbankgeld zu leihen, und um so weniger Geld gerät in Umlauf; umgekehrt sorgen niedrige Zinsen für eine hohe Geldmenge. Um die Akkumulation des fiktiven Kapitals nach der Krise von 2008 wieder in Gang zu bringen, sahen sich

[43] In der Tat tendieren die Gestehungskosten des Bitcoins schon jetzt dahin, höher zu werden als ihr derzeit gehandelter Preis (siehe Hecking 2018).

die Notenbanken jedoch gezwungen, die Leitzinsen auf Werte um und unter 0 % zu senken. Damit ist bereits eine umfassende Entwertung des Zentralbankgeldes vorbereitet. Außerdem waren noch weitere drastische Maßnahmen erforderlich, um einen Krisenverlauf, der in seiner Schwere den Verlauf der Weltwirtschaftskrise von 1929 zu übertreffen drohte, zu verhindern. Dazu gehörte zum einen die Senkung der Bonitätsstandards für die Herausgabe von Zentralbankgeld. Das bedeutet nichts anderes, als dass die Wertpapiere, die im Gegenzug für die Herausgabe des Zentralbankgeldes entgegengenommen wurden, von immer zweifelhafterem Ruf waren und sind, was wiederum eine Verschlechterung der in den Zentralbanktresoren eingelagerten Geldware bedeutet. Zum anderen kam noch die Neuerung hinzu, dass die Zentralbanken dazu übergingen, massenhaft Staatsanleihen aufzukaufen, und zwar in erheblichem Maße auch solche von hochverschuldeten Staaten wie etwa Griechenland oder Italien. Das wurde allgemein als Verstoß gegen bis dahin geltende Spielregeln aufgefasst. Wenn aber die Zentralbanken Papiere aufkaufen, die mit einem hohem Verlustrisiko behaftet sind, dann steigert das in einem hohen Maße die Gefahr, dass Teile der Geldware komplett wertlos werden und somit einen Totalverlust erleiden.

In der Tat beruhen etliche der in den Notenbanken eingelagerten Geldwaren (sprich: Wertpapieren) mittlerweile auf Wertschöpfungserwartungen, die absehbar niemals erfüllt werden. In diesem Sinne ist ein signifikanter Anteil der in Umlauf befindlichen Geldzeichen faktisch ungedeckt. Insofern kann man es durchaus als Menetekel auffassen, dass im Januar 2009 – also kurz nach Beginn der Finanzkrise, in deren Verlauf die Deckung des Zentralbankgeldes zunehmend fadenscheiniger wird – mit dem Bitcoin die erste Kryptowährung auftritt, die sich ja gerade dadurch auszeichnet, dass sie keinerlei Deckung aufweist. Dass Bitcoin und seine Verwandten tatsächlich an die Stelle von Zentralbankgeld treten könnten, wie es ihre Erfinder meinten, bleibt zwar eine ideologische Flause, aber das Zentralbankgeld ist den Kryptowährungen im Zuge der Krise ähnlicher geworden, als es EZB, FED und Co. lieb sein dürfte.

Gleichzeitig werden die gängigsten Kryptowährungen aber auch zunehmend in das allgemeine Finanzsystem eingebunden und zu Bezugspunkten für die

Bildung von fiktivem Kapital. So startete etwa die US-Börse CNE im Dezember 2017 den Handel mit Bitcoin-Futures; die US-Technologiebörse Nasdaq zog kurz darauf nach. Damit ist den betreffenden Kryptowährungen der Anschluss an den allgemeinen Wertpapierhandel gelungen (Landgraf 2018, S. 2). Eine weitere Verschränkung von Kryptowährungen mit der landläufigen Finanzwirtschaft stellt die »Tokenisierung« dar. Tokenisierung bedeutet, das Vermögenswerte wie Aktien, Anleihen, Immobilien, Gold etc. auf eine Blockchain gebracht und dort gehandelt werden (Hosp 2018, S. 151). Beide Entwicklungen erhöhen die Gefahr, dass die extreme Volatilität der Kryptowährungen die Instabilität des Finanzsystems verstärken und sogar einen neuen Krisenschub auslösen könnte. Das wäre aber das genaue Gegenteil des Anspruchs, den Satoshi Nakamoto kurz nach der Finanzkrise von 2008 erhob, als er den Bitcoin entwickelte.

Literatur

Bitcoin Deutschland AG: Allgemeine Geschäftsbedingungen. www.bitcoin.de/de/agb

Born, Karl Erich (1977): Geld und Banken im 19. und 20. Jahrhundert, Stuttgart 1977

Flassbeck, Heiner; Spiecker, Friederike (2007): Das Ende der Massenarbeitslosigkeit. Frankfurt am Main 2007

Hecking, Claus (2018): Bitcoin Experte: „Das Bitcoin-System verbraucht mehr Strom als die Schweizer Volkswirtschaft". In: www.spiegel.de/wirtschaft/unternehmen/bitcoin-energieverbrauch-fuer-produktion-und-verwaltung-a-1208635.html22.05.2018

Heise, Arne (2018): Kein Raum für Dogmen an Unis. In: Frankfurter Rundschau 16.05.2018, S. 10

Hickel, Rudolf (2017): Bitcoins helfen nur Spekulanten. In: Frankfurter Rundschau 01.12.2017, S. 12

Hosp, Julian (2018): Kryptowährungen. Bitcoin, Ethereum, ICOs & Co. einfach erklärt. München 2018

Junge Linke (2012): Bitcoin – endlich ein faires Geld? www.streifzuege.org/2012/bitcoin-endlich-faires-geld, 29.04.2012

Kaufmann, Stefan (2017): Nichts als Spekulation. In: Frankfurter Rundschau 23.11.2017a, S. 16

Klein, Dominik (2018): Der digitale Goldrausch. https://jungle.world/artikel/2018/04/der-digitale-goldrausch

Landgraf, Anton (2018): New Kids on the Blockchain. In: jungle world 04/2018, https://jungle.world/print/pdf/node/58404/debug

Lohoff, Ernst (2018): Die allgemeine Ware und ihre Mysterien. Zur Bedeutung des Geldes in der Kritik der politischen Ökonomie, Krisis 2/2018, www.krisis.org

Lohoff, Ernst (2014): Kapitalakkumulation ohne Wertverwertung, Krisis 1/2014, www.krisis.org/2014/kapitalakkumulation-ohne-wertakkumulation/

Lohoff, Ernst; Trenkle, Norbert (2012): Die große Entwertung. Münster 2012

Marx, Karl (1988): Das Kapital Bd. 3. Berlin 1988 [1894]

Mayer-Kuckuk, Finn (2017): „Die Party ist vorbei”. In: Frankfurter Rundschau 12.12.2017, S. 15

Müller, Rudolf Wolfgang (1981): Geld und Geist. Frankfurt/New York 1981 [1977]

Ortlieb, Claus Peter (2014): Bitte ein Bitcoin. In: Konkret 3/2014, auch unter dem Titel „Digitale und andere Blüten. Was die Karriere des Bitcoins über den Zustand des Geldmediums verrät.“ auf `www.exit-online.org/textanz1.php?tabelle=aktuelles&index=0&posnr=605`

Schulz, Hajo (2017a): Das macht Blockchain. Die Technik hinter Bitcoin und Co. In: c't, Heft 23/ 2017, S. 102-106

Schulz, Hajo (2017b): Vertrag denkt mit. Smart Contracs in der Ethereum-Blockchain. In: c't, Heft 23/ 2017, S. 108-112

Voß, Malte (2018): „Bei Bitcoin geht es weniger um Technologie als um Psychologie. `https://jungle.world/artikel/2018/04/bei-bitcoin-geht-es-weniger-um-technologie-als-um-psychologie`

Wille, Joachim (2017): Umweltfrevel Bitcoin. In: Frankfurter Rundschau 02.12.2017, S. 16

Krisis – Kritik der Warengesellschaft

Krisis Beiträge seit 2013:

1 / 2013 Peter Samol

Michael Heinrichs Fehlkalkulationen der Profitrate

Zur Widerlegung von Michael Heinrichs »Kritik am Gesetz vom tendenziellen Fall der Profitrate« und über die Bedeutung der schrumpfenden Wertmasse für den Krisenverlauf

2 / 2013 Ernst Lohoff

Auf Selbstzerstörung Programmiert

Über den inneren Zusammenhang von Wertformkritik und Krisentheorie in der Marxschen Kritik der Politischen Ökonomie

3 / 2013 Julian Bierwirth

Gegenständlicher Schein

Zur Gesellschaftlichkeit von Zweckrationalität und Ich-Identität

4 / 2013 Peter Samol

Ein theoretischer Holzweg

Die seltsame Fassung des Begriffs der »unproduktiven Arbeit« von Robert Kurz und wie er sich als Reaktion auf die Kritik daran in einen noch tieferen Schlamassel begeben hat

1 / 2014 Ernst Lohoff

Kapitalakkumulation ohne Wertakkumulation

Der Fetischcharakter der Kapitalmarktwaren und sein Geheimnis

1 / 2015 Julian Bierwirth

Henne und Ei

Der Wert als Einheit von Handlung und Struktur

1 / 2016	Norbert Trenkle **Die Arbeit hängt am Tropf des fiktiven Kapitals** Eine Antwort auf »*Geht dem Kapitalismus die Arbeit aus?*« von Christian Siefkes	
2 / 2016	Julian Bierwirth **Der Grabbeltisch der Erkenntnis** Untersuchung zur Methode des *Gegenstandpunkt*	
3 / 2016	Karl-Heinz Lewed **Rekonstruktion oder Dekonstruktion?** Über die Versuche von Backhaus und der Monetären Werttheorie, den Wertbegriff zu rekonstruieren	
4 / 2016	Peter Samol **All the Lonely People** Narzissmus als adäquate Subjektform des Kapitalismus	
5 / 2016	Ernst Lohoff **Die letzten Tage des Weltkapitals** Kapitalakkumulation und Politik im Zeitalter des fiktiven Kapitals	
1 / 2018	Peter Samol **Bitcoinblase und Blockchainballyhoo** Warum Bitcoin und andere Kryptowährungen kein Geld darstellen und dieses auch nicht ersetzen können	

Das komplette Archiv der Krisis seit 1986 findet sich auf www.krisis.org
Ein Teil der Druckausgaben ist noch erhältlich und kann bei u.a. Adresse bestellt werden.

Förderverein Krisis | Postfach 81 02 69 | 90247 Nürnberg | krisisweb@yahoo.de

k